Política de seguridad recomendada para el centro de datos

Version 10.0 (EoL)

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

November 2, 2020

Table of Contents

Lista de verificación de la política de seguridad recomendada para el centro de datos

Los activos más valiosos de su empresa residen en su centro de datos, lo que incluye el código fuente exclusivo, la propiedad intelectual y los datos confidenciales de la empresa y el cliente. Sus clientes y empleados confían en que garantizará la confidencialidad y la integridad de sus datos, y esperan que los datos siempre estén disponibles, de modo que es esencial implementar una política de seguridad recomendada para el centro de datos que proteja sus datos y evite ataques exitosos. No es suficiente reforzar el perímetro de la red debido a que los ataques pueden originarse en el interior de la red, los ataques pueden provenir de socios o contratistas cuyas credenciales se encuentren en riesgo, y debido a que si un atacante logra establecerse en su red, podrá atacar desde el interior sin moverse lateralmente desde dispositivo a dispositivo.

Si conoce la plataforma de Palo Alto Networks, puede ahorrar tiempo usando la lista de verificación optimizada para implementar la política de seguridad recomendada para el centro de datos en la implementación previa, la implementación y la implementación posterior. Cada sección incluye enlaces a información detallada en el documento completo acerca de la política de seguridad recomendada para el centro de datos o en la Guía de administración de PAN-OS 10.0, que incluye cómo configurar reglas de la política y perfiles de seguridad.

- Planifique la implementación recomendada para el centro de datos
- Implementación de prácticas recomendadas para el centro de datos
- Respeto de las prácticas recomendadas para el centro de datos tras la implementación

Planifique la implementación recomendada para el centro de datos

Prepárese para implementar las prácticas recomendadas en el centro de datos con una estrategia y un plan de implementación. Use la aplicación positiva de seguridad (cree reglas que permitan el tráfico de usuario y de aplicación que desea permitir, y bloquee el resto) para desarrollar una arquitectura de Zero Trust.

STEP 1 | Establezca objetivos.

- ❑ Defina el estado ideal para el futuro de la red del centro de datos, de modo que cuente con objetivos definitivos a fin de trabajar para lograrlos y saber cuándo lo ha hecho.
- ❑ Proteja los flujos de tráfico de cada área en las que inician las conexiones:
  1. Flujo del tráfico de usuario local hacia el centro de datos.
  2. Tráfico que fluye desde internet hacia el centro de datos.
  3. Tráfico que fluye desde el centro de datos hacia internet.
  4. Tráfico que fluye entre los servidores o VM en el centro de datos (tráfico horizontal en el centro de datos).
- ❑ No permita usuarios, aplicaciones o tráfico desconocido en el centro de datos.
- ❑ Cree un diseño estándar escalable que pueda replicar y aplicar de manera uniforme en los centros de datos.

STEP 2 | Trabaje con las partes interesadas, como el equipo de TI/asistencia técnica, de seguridad y los grupos de requieran acceso al centro de datos, como los departamentos de ingeniería, jurídico, finanzas y RR. HH., para desarrollar una estrategia de acceso.

- ❑ Identifique a los usuarios que requieran acceso y los activos a los que desean acceder. Comprenderlo le permite crear grupos de usuarios basados en los requisitos del nivel de acceso, de modo que pueda diseñar reglas eficientes en la política de seguridad según el grupo de usuario.
- ❑ Identifique las aplicaciones que desea permitir (sancionar) en el centro de datos. Para reducir la superficie de ataque, sancione aplicaciones únicamente por motivos empresariales legítimos.

STEP 3 | Evalúe el centro de datos para comprender su estado actual, de modo que pueda crear un plan para transformar la seguridad del centro de datos al estado deseado para el futuro.

- ❑ Realice un inventario del entorno físico y virtual, y de los activos, que incluya lo siguiente:
  - ❑ Servidores, enrutadores, conmutadores, dispositivos de seguridad, equilibradores de carga y otra infraestructura de red.
  - ❑ Aplicaciones personalizadas estándar y exclusivas, y las cuentas de servicio que usan para comunicarse. Compare la lista del inventario de aplicaciones con la lista de aplicaciones de desea sancionar.

    Céntrese en las aplicaciones que desea permitir dado que las reglas de la política de seguridad de la lista de permitidos las permiten y, de manera predeterminada, bloquea el resto de las aplicaciones para reducir la superficie de ataque. Asigne aplicaciones a requisitos empresariales. Si una aplicación no se asigna a un requisito empresarial, evalúe si debería permitirla.
  - ❑ Evalúe cada activo para establecer una prioridad de cuáles desea proteger primero. Pregúntese "¿Qué define y diferencia a su empresa?", "¿Qué sistemas deben estar disponibles para las operaciones diarias?" y "Si pierdo este activo, ¿cuáles son las consecuencias?"

- ❑ Trabaje con arquitectos de aplicaciones, redes y empresas, y con representantes del negocio para caracterizar los flujos de tráfico del centro de datos y obtener información sobre las cargas y los patrones de tráfico de referencia habituales, de modo que pueda comprender el comportamiento habitual de la red. Use los widgets y las herramientas de análisis de tráfico del centro de control de aplicaciones para establecer una referencia del tráfico.

STEP 4 | Cree una estrategia de segmentación de centro de datos para evitar que el malware que se establezca en el centro de datos se mueva lateralmente para infectar otros sistemas.

- ❑ Use cortafuegos como puertas de enlace de segmentación para ofrecer visibilidad del tráfico y los sistemas del centro de datos, de modo que pueda controlar con mayor detalle quién puede usar las aplicaciones para acceder a cada dispositivo. Segmente y proteja servidores no virtualizados con cortafuegos físicos y la red virtual con cortafuegos serie VM.
- ❑ Use las herramientas de segmentación flexibles del cortafuegos como las zonas, los grupos de direcciones dinámicas, App-ID y User-ID para diseñar una estrategia de segmentación detallada que proteja servidores y datos confidenciales.
- ❑ Agrupe activos que funcionen de manera similar y requieran el mismo nivel de seguridad en el mismo segmento.
- ❑ Segmente las aplicaciones del centro de datos segmentando los niveles de servidor que conforman el nivel de aplicación (por lo general, una cadena de servicio compuesta por un nivel de servidor web, un nivel de servidor de la aplicación y un nivel de servidor de la base de datos) y usando el cortafuegos para controlar e inspeccionar el tráfico entre los niveles.
- ❑ Considere usar una solución de SDN en el centro de datos para obtener una infraestructura ágil y virtualizada que maximiza el uso de los recursos y facilita la automatización y la escala.

STEP 5 | Planifique usar la metodología recomendada para inspeccionar todo el tráfico del centro de datos y obtener visibilidad completa, reducir la superficie de ataque y evitar amenazas conocidas y desconocidas.

- ❑ Ubique cortafuegos físicos y virtuales donde puedan ver todo el tráfico de la red del centro de datos.
- ❑ Aproveche el conjunto de herramientas potente del cortafuegos para crear reglas basadas en la aplicación en la política de seguridad vinculadas a grupos de usuarios específicos y protegidas con perfiles de seguridad. Reenvíe los archivos desconocidos a WildFire e implemente el descifrado para evitar que las amenazas accedan al centro de datos en tráfico cifrado.
- ❑ Use GlobalProtect en modo interno como una puerta de enlace para controlar el acceso al centro de datos.
- ❑ Autentique a los usuarios para evitar el acceso no autorizado y configure la autenticación multifactor para conceder el acceso a las aplicaciones, servicios y servidores confidenciales, en especial, a contratistas, socios y terceros que desean acceder al centro de datos.
- ❑ Gestione los cortafuegos de manera centralizada con Panorama para aplicar una política uniforme en los entornos físicos y virtuales, y obtener visibilidad centralizada.
- ❑ Si tiene varios centros de datos, vuelva a usar las plantillas y las pilas de plantillas para aplicar una política de seguridad uniforme en todas las ubicaciones.

STEP 6 | Incorpore la implementación recomendada con el tiempo; comience centrándose en las amenazas más probables para su negocio y red, y proteja los activos más valiosos primero.

Tener en cuenta a los usuarios, las aplicaciones y los dispositivos y los flujos de tráfico del centro de datos, y crear una política de seguridad recomendada puede parecer una tarea abrumadora si intenta hacerlo a la vez. Pero si protege los activos más valiosos primero y planifica una implementación gradual y progresiva, puede realizar la transición de manera fluida y práctica desde una política de seguridad confiada a una política de seguridad recomendada que le permita habilitar aplicaciones, usuarios y contenido de manera segura.

Implementación de prácticas recomendadas para el centro de datos

Implemente las prácticas recomendadas para el centro de datos cuando crea perfiles de seguridad, perfiles de descifrado, reglas en la política de seguridad, reglas en la política de autenticación y reglas en la política de descifrado.

En las reglas de seguridad, autenticación y las reglas en la política de DoS, configure el reenvío de logs *a Panorama o servicios externos para centralizar los logs a fin de visualizarlos y analizarlos de manera conveniente con notificaciones.*

- Objetos, políticas y acciones del centro de datos global
- Políticas de tráfico del centro de datos del usuario
- Políticas de tráfico de Internet al centro de datos
- Políticas de tráfico del centro de datos a Internet
- Políticas de tráfico en el centro de datos
- Orden de la base de reglas de la política de seguridad del centro de datos

Objetos, políticas y acciones del centro de datos global

Asegúrese de poder proteger las aplicaciones personalizadas si las usa. Configure los perfiles de seguridad y los perfiles de descifrado e instale el agente Cortex XDR en todos los endpoints del centro de datos.

- Aplicaciones personalizadas
- Perfiles de seguridad
- Perfiles de descifrado
- Reglas de bloqueo de tráfico
- Instalar Cortex XDR Agent en los endpoints

STEP 1 | Si su inventario de aplicaciones en el centro de datos incluye aplicaciones exclusivas personalizadas, cree aplicaciones personalizadas para ellas, de modo que pueda especificarlas en la política de seguridad.

STEP 2 | Configure perfiles de seguridad estrictos recomendados para el centro de datos para evitar que las amenazas perjudiquen a la red del centro de datos.

- ❑ Configure el perfil de antivirus recomendado clonando el perfil predefinido y cambiando los valores del decodificador imap, pop3 y smtp a **reset-both (restablecer ambos)** en las columnas Action (Acción) y WildFire Action (Acción de WildFire).
- ❑ Configure el perfil antispyware recomendado clonando el perfil estricto predefinido. En la pestaña **Rules (Reglas)**, habilite la captura de paquetes única para las amenazas de gravedad media, alta y crítica en el tráfico que registra. (En el tráfico que no registra, aplique un perfil diferente sin captura de paquetes).

  En la pestaña DNS Signatures (Firmas DNS), cambie la **Action (Acción)** en DNS Queries (Solicitudes DNS) a **sinkhole** si el cortafuegos no ve el creador de la solicitud DNS (por lo general, cuando el cortafuegos se encuentra antes del servidor DNS local), de modo que pueda identificar los hosts infectados. Sinkhole DNS identifica y realiza el seguimiento de hosts potencialmente en riesgo que

intentan acceder a dominios sospechosos y evita que accedan a esos dominios. Habilite la captura de paquetes amplia en el tráfico con sinkhole.

- Configure el perfil de protección contra vulnerabilidades recomendado clonando el perfil estricto predefinido y cambiando el ajuste de captura de paquetes en cada regla, a excepción de **simple-client-informational** y **simple-server-informational** a **single-packet (paquete único)**. Si el cortafuegos identifica un gran volumen de amenazas de vulnerabilidad que afecta al rendimiento, deshabilite la captura de paquetes en los eventos de gravedad leve.
- El perfil de bloqueo de archivos estricto predefinido es el perfil recomendado. Si admitir aplicaciones críticas evita que bloquee todos los tipos de archivos que bloquea el perfil estricto [puede identificar los tipos de archivos que se usan en el centro de datos en los logs de filtrado de datos en **Monitor (Supervisar)** > **Logs** > **Data Filtering (Filtrado de datos)**], clone el perfil estricto y modifíquelo según sea necesario. Si los archivos no necesitan moverse en ambas direcciones, use el ajuste **Direction (Dirección)** para limitar el tipo de archivo a la dirección necesaria.
- El perfil de análisis de WildFire predefinido es el perfil recomendado. WildFire ofrece la mejor defensa contra las amenazas desconocidas y las amenazas avanzadas persistentes (advanced persistent threats, ATP).

STEP 3 | Configure perfiles de descifrado recomendados estrictos para el centro de datos para evitar que tráfico desconocido acceda al centro de datos.

- Realice comprobaciones de CRL/OCSP para garantizar que los certificados que se presentan durante el descifrado SSL sean válidos.
- Ajustes de protocolo SSL: Configure **Min Version (Versión mínima)** en **TLSv1.2**, **Max Version (Versión máxima)** en **Max** y elimine la marca del algoritmo de autenticación **SHA1**. (La selección de los algoritmos de cifrado débil 3DES y RC4 se elimina automáticamente cuando selecciona TLSv1.2.) Utilice TLSv1.3 para el tráfico que admite TLSv1.3 (muchas aplicaciones móviles usan la fijación de certificados, lo que evita el descifrado cuando se usa TLSv1.3, por tanto, para estas aplicaciones, use TLSv1.2).
- Proxy SSL de reenvío: Para realizar la **Server Certificate Verification (Verificación del certificado de servidor)**, bloquee sesiones con certificados vencidos, emisores no fiables y estados de certificado desconocidos, y limite las extensiones de los certificados. Para realizar las **Unsupported Mode Checks (Comprobaciones de modo no admitidas)**, bloquee las sesiones con versiones no admitidas, conjuntos de cifrado no admitidos y autenticación de cliente. En el caso de las **Failure Checks (Comprobaciones de fallos)**, bloquear las sesiones si los recursos no están disponibles es una compensación entre la experiencia del usuario (es posible que el bloqueo afecte la experiencia del usuario de manera negativa) y la posibilidad de permitir conexiones peligrosas. Si debe considerar esta compensación, también considere aumentar los recursos de descifrado disponibles en la implementación.
- Inspección entrante de SSL: Para realizar las **Unsupported Mode Checks (Comprobaciones de modo no admitidas)**, bloquee las sesiones con versiones y cifrados no admitidos. En el caso de las **Failure Checks (Comprobaciones de fallos)**, las compensaciones son similares a las del proxy SSL de reenvío.
- Proxy SSH: Para realizar las **Unsupported Mode Checks (Comprobaciones de modo no admitidas)**, bloquee las sesiones con versiones y algoritmos no admitidos. En el caso de las **Failure Checks (Comprobaciones de fallos)**, las compensaciones son similares a las del proxy SSL de reenvío.
- Aplique el perfil Sin descifrado al tráfico que decida no descifrar por motivos de regulación, normas de cumplimiento o razones comerciales; excepto el tráfico TLSv1.3 (TLSv1.3 cifra la información del certificado, por lo que el cortafuegos no puede bloquear el tráfico en función de la información certificada). Bloquee las sesiones con certificados vencidos y emisores no fiables.

STEP 4 | Configure las reglas de bloqueo de tráfico para bloquear el tráfico que sepa que es malintencionado o que no es necesario por motivos empresariales.

Es posible que la generación de logs y la supervisión de las reglas de bloqueo revelen usuarios y aplicaciones que no sabía que se encontraban en la red, y que pueden ser legítimos o indicar un ataque. El orden de las reglas en la base de reglas de la política de seguridad es crítica para evitar el *enmascaramiento* (tráfico que coincide con una regla de permiso o bloqueo antes de que coincida con

la regla con la que desea que coincida el tráfico). Algunas reglas son muy similares, pero permiten la creación de informes separados para puertos estándar y no estándar, o para aplicaciones de usuario y aplicaciones de otros orígenes. En cada regla, configure **Log at Session End (Log al finalizar sesión)** en la pestaña **Actions (Acciones)** y establezca el reenvío de logs para realizar el seguimiento y analizar los incumplimientos de la regla.

- Bloquee todas las aplicaciones de zonas de usuario en el puerto **application-default**. Ubique esta regla *después* de las reglas que permiten tráfico de aplicaciones legítimas de zonas de usuario para identificar aplicaciones de usuario desconocidas o inesperadas en puertos estándar.

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-from-User-Zone	User to DC BP	universal	Contractors Engineering-Users Finance-Users IT-Users	any	any	any	Web-Server-Tier-DC	any	any	any	application-default	Drop	none	

- Bloquee todas las aplicaciones de las zonas de usuario en **any (cualquier)** puerto para captar el tráfico de usuario que intente usar puertos no estándar. Ubique esta regla después de la regla de bloqueo **application-default** anterior para identificar aplicaciones de usuario desconocidas o inesperadas en puertos no estándar, que puedan ser aplicaciones personalizadas o evasivas.

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-User-App-Any-Port	User to DC BP	universal	Contractors Engineering-Users Finance-Users IT-Users	any	any	any	Web-Server-Tier-DC	any	any	any	any	Drop	none	

- Bloquee las aplicaciones que *no* desea en el centro de datos, como aplicaciones evasivas, aplicaciones habitualmente vulnerables y aplicaciones que no son necesarias para el negocio. Coloque esta regla después de las reglas de aplicaciones permitidas, de modo que, por ejemplo, permita aplicaciones sancionadas de uso compartido de archivos antes de que **Filesharing** bloquee el resto de las aplicaciones de uso compartido de archivos.

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Block-Bad-Apps	User to DC BP	universal	any	any	any	any	App-Server-Tier-DC DB-Server-Tier-DC Engineering-DC-Infra Finance-DC-Infra IT Infrastructure SAP-Infra Web-Server-Tier-DC	any	any	Encrypted-Tunnels File-Sharing Remote-Access	any	Drop	none	

- Bloquee todas las aplicaciones de **any (cualquier)** zona en el puerto **application-default** para identificar aplicaciones inesperadas en puertos estándar. Las coincidencias de reglas pueden indicar posibles amenazas o cambios en la aplicación que requieren la modificación de una regla de permiso. Ubique esta regla después de las reglas de aplicaciones permitidas y la regla de bloqueo que le precede.

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-from-Any-Zone	universal	any	any	any	any	Web-Server-Tier-DC	any	any	any	application-default	Drop	none	

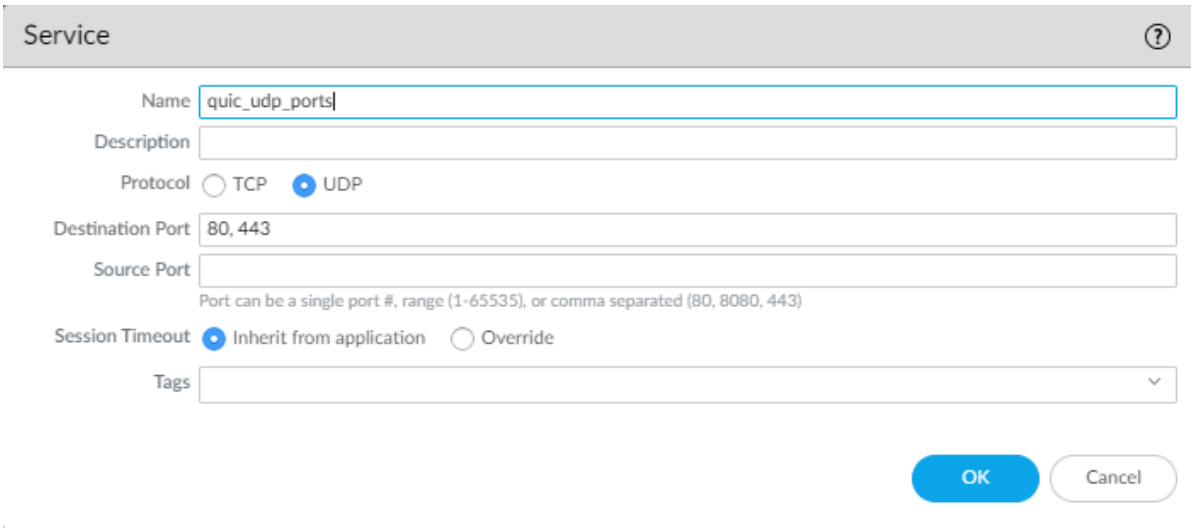
- Bloquee todas las aplicaciones de cualquier zona en **any (cualquier)** puerto para identificar las aplicaciones inesperadas en puertos no estándar. No permita tráfico unknown-tcp, unknown-udp o non-syn-tcp. Ubique esta regla después de las reglas de aplicaciones permitidas y la regla de bloqueo que le precede.

NAME	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
		ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Unexpected-App-Any-Port	universal	any	any	any	any	Web-Server-Tier-DC	any	any	any	any	Drop	none	

- Bloquee los usuarios *desconocidos* que intenten ejecutar aplicaciones en cualquier puerto para hallar a los usuarios desconocidos (brechas en la cobertura de User-ID o atacantes) e identificar los dispositivos en riesgo (incluso los dispositivos integrados como impresoras, lectores de tarjetas y cámaras). Ubique esta regla después de las reglas de aplicaciones permitidas y la regla de bloqueo que le precede.

NAME	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
		ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Discover-Unknown-Users	universal	any	any	unknown	any	any	any	any	any	any	Deny	none	

- Además de bloquear el tráfico potencialmente malintencionado no deseado, bloquee el protocolo de Conexiones UDP rápidas en Internet (QUIC), a menos que por motivos comerciales desee permitir el tráfico cifrado del navegador. Chrome y algunos otros exploradores establecen sesiones con QUIC en lugar de TLS, pero QUIC usa cifrado de propiedad que el cortafuegos no puede descifrar, por lo que tráfico potencialmente peligroso puede entrar en la red como tráfico cifrado. Bloquee tanto la aplicación QUIC como los puertos UDP 80 y 443 para forzar al navegador a utilizar TLS. Primero cree un servicio [**Objects (Objetos)** > **Services (Servicios)**] que incluya los puertos UDP 80 y 443:



Utilice el servicio para especificar los puertos UDP que se bloquearán para QUIC. En la segunda regla, bloquee la aplicación QUIC para que las dos primeras reglas de su base de reglas bloqueen QUIC:

	NAME	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
1	Block QUIC UDP	universal	l3-vlan-trust	any	any	any	l3-untrust	any	any	any	quic_udp_ports	Deny	none	
2	Block QUIC	universal	l3-vlan-trust	any	any	any	l3-untrust	any	any	quic	application-default	Deny	none	

STEP 5 | Instale Cortex XDR Agent en todos los endpoints del centro de datos para protegerse contra malware y vulnerabilidades de seguridad en los endpoints.

Cortex XDR Agent protege todos los endpoints de la misma manera, de modo que el proceso de implementación y las prácticas recomendadas para la política de protección frente a malware son las mismas para el centro de datos y otras áreas de la red.

Políticas de tráfico del centro de datos del usuario

Configure la política de seguridad, la política de autenticación y la política de descifrado para los usuarios que necesitan acceder al centro de datos.

- Reglas de la política de seguridad de usuarios
- Reglas de la política de autenticación de usuarios
- Reglas de la política de descifrado de usuarios

STEP 1 | Cree reglas de política de seguridad de la lista de aplicaciones permitidas para que el tráfico de usuario permita el acceso adecuado.

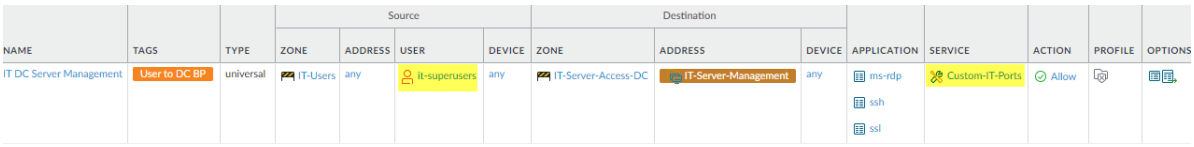
Coloque las reglas de permiso para el acceso de usuarios en la parte superior de la base de reglas, antes de las reglas de bloqueo, para evitar bloquear tráfico legítimo accidentalmente. En cada regla, configure **Log at Session End (Log al finalizar sesión)** en la pestaña **Actions (Acciones)** y establezca el reenvío de logs para realizar el seguimiento y analizar los incumplimientos de la regla.

- Habilite el acceso de usuarios empleados a servidores DNS corporativos internos. Esta regla permite a cualquier usuario porque los usuarios acceden a los servicios DNS antes de iniciar sesión. La regla controla de manera estricta la zona de origen, los servidores de destino y la aplicación, y aplica perfiles de seguridad al tráfico.

  Bloquee el acceso a servidores DNS externos en la puerta de enlace de internet para evitar que el tráfico DNS se dirija a internet y a servidores públicos.

- Permita que el personal de TI necesario obtenga acceso privilegiado y seguro a las interfaces de gestión del centro de datos. Restrinja la regla a las interfaces de gestión (este ejemplo usa un grupo de direcciones para identificar los dispositivos y un servicio personalizado para identificar los puertos de gestión) y las aplicaciones necesarias, en este ejemplo, RDP, SSH y SSL. Use una VLAN dedicada para separar el tráfico de gestión de otro tráfico y ubique las interfaces de gestión en la misma subred.

  Si el mismo grupo de usuarios de TI gestiona los conmutadores, los enrutadores y otros dispositivos del centro de datos, añádalos al destino y añada sus puertos al servicio personalizado, de modo que la regla proteja el tráfico en las conexiones a sus interfaces de gestión. Si diferentes grupos de TI gestionan diferentes recursos del centro de datos, cree reglas diferentes en la política de seguridad y las reglas en la política de descifrado y la política de autenticación correspondientes a cada grupo.



- Permita el acceso necesario a los grupos de usuarios empleados. Estas reglas limitan el acceso de cada grupo de usuarios (o usuario) a las aplicaciones y servidores necesarios. En este ejemplo, se limita el acceso de un grupo de usuarios de ingeniería únicamente a los servidores y aplicaciones de desarrollo.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Engineering Resources	User to DC BP	universal	Engineering-Users	any	api-users engg-users	any	Engineering-DC-Infra	Dev-Servers	any	oracle-bi perforce profinet qlikview	application-default	Allow		

- Permita acceso limitado y específico a contratistas, socios, clientes y terceros. En este ejemplo, se limita el acceso de un grupo de contratistas de SAP, de modo que el grupo solo pueda acceder a los servidores de la base de datos de SAP adecuados usando únicamente las aplicaciones adecuadas.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
SAP-Contractors	User to DC BP	universal	Contractors	any	sap-contractors	any	SAP-Infra	SAP DB Servers	any	ms-sql-analysis-service mssql-db mssql-mon sap	application-default	Allow		

STEP 2 | Cree reglas en la política de autenticación para el tráfico de usuarios para autenticar el acceso al centro de datos.

Para cada grupo de usuarios o usuarios para los que crea reglas de aplicaciones permitidas, cree una regla análoga de autenticación (a excepción de la regla de permiso de DNS, ya que DNS se ejecuta antes de que los usuarios se autentiquen para iniciar sesión). En cada regla, configure **Log at Session End (Log al finalizar sesión)** en la pestaña **Actions (Acciones)** y establezca el reenvío de logs para realizar el seguimiento y analizar los incumplimientos de la regla.

- Autentique a los usuarios que requieren acceso especializado. Este ejemplo autentica al personal de TI que requiere acceso privilegiado seguro para gestionar servidores del centro de datos de la regla de permiso del paso anterior. Debido a que poner en riesgo las credenciales de un usuario privilegiado permite que el atacante acceda al centro de datos, requiera autenticación multifactor (Multi-Factor Authentication, MFA) para protegerse de las credenciales robadas.

Si el mismo grupo de usuarios de TI gestiona los conmutadores, los enrutadores y otros dispositivos del centro de datos, añádalos al destino y añada sus puertos al servicio personalizado, de modo que la regla autentique el tráfico en las conexiones a sus interfaces de gestión. Si diferentes grupos de TI gestionan diferentes recursos del centro de datos, cree reglas diferentes en la política de seguridad y las reglas en la política de descifrado y la política de autenticación correspondientes a cada grupo.

NAME	TAGS	Source				Destination			SERVICE	AUTHENTICATION ENFORCEMENT	LOG SETTINGS
		ZONE	ADDR...	USER	DEVI...	ZONE	ADDRESS	DEVI...			
IT Secured Access	User to DC BP	IT-Users	any	it-superusers	any	IT-Server-Access-DC	IT-Server-Management	any	Custom-IT-Ports	Auth-IT-Server-Mgmt	Log Authentication Timeouts: yes Log Forwarding: Auth-LF

- Autentique a los empleados con motivos empresariales legítimos para que accedan al centro de datos. Este ejemplo autentica el grupo de usuarios de desarrollo de ingeniería de la regla de permisos del paso anterior.

NAME	TAGS	Source				Destination			SERVICE	AUTHENTICATION ENFORCEMENT	LOG SETTINGS
		ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			
DevEng Resources	User to DC BP	Engineering-Users	any	api-users engg-users	any	Engineering-DC-Infra	Dev-Servers	any	Perforce rdp service-http service-https ssh	Auth-Dev-Servers	Log Authentication Timeouts: yes Log Forwarding: Auth-LF

- Autentique a contratistas, socios, clientes y otros grupos de no empleados. Requiera MFA en los grupos sin empleados para protegerse contra el robo de credenciales en una empresa externa. Este ejemplo autentica a desarrolladores de SAP de la regla de permiso del paso anterior.

NAME	TAGS	Source				Destination			SERVICE	AUTHENTICATI... ENFORCEMENT	LOG SETTINGS
		ZONE	ADDR...	USER	DEVI...	ZONE	ADDRESS	DEVI...			
SAP Resources	User to DC BP	Contractors	any	sap-contractors	any	SAP-Infra	SAP DB Servers	any	SAP-Services service-http service-https	Auth-SAP-Servers	Log Authentication Timeouts: yes Log Forwarding: Auth-LF

STEP 3 | Cree reglas en la política de descifrado para el tráfico de usuario para descifrar el tráfico que permite, de modo que el cortafuegos pueda ver, inspeccionar y aplicar la política de seguridad al tráfico.

Para cada regla de la política de descifrado, aplique el perfil de descifrado recomendado adecuado (Inspección entrante de SSL, Proxy SSL de reenvío, Proxy SSH o Sin descifrado, que incluye los ajustes de protocolo SSL recomendados para la inspección entrante de SSL y las reglas de proxy SSL de reenvío) para bloquear protocolos y algoritmos débiles, y para verificar los certificados de servidor. Para cada regla de inspección entrante de SSL, importe el certificado del servidor del centro de datos que protege con descifrado.

Excluya tráfico del descifrado *únicamente por estos dos motivos:*

- *El tráfico anula el descifrado debido a motivos técnicos, como un certificado anclado o una autenticación mutua. Añada exclusiones técnicas a la lista Device (Dispositivo) > Certificate Management (Gestión de certificados) > SSL Decryption Exclusion (Exclusión de descifrado SSL).*
- *Tráfico que decide no descifrar debido a motivos empresariales, de reglamentación, de cumplimiento o de otro tipo, como el tráfico de finanzas, salud o gobierno. Cree exclusiones del descifrado basadas en la política para el tráfico que decide no descifrar.*

- Descifre el tráfico de la regla creada previamente en la política de seguridad que permite acceso privilegiado de TI a los servidores de gestión. La regla de la política de descifrado y el perfil de descifrado asociado varían en función de si el grupo de TI usa SSL (perfil de descifrado de proxy SSL de reenvío) o SSH (perfil de descifrado de proxy SSH) para acceder a los puertos de gestión.

  Si el mismo grupo de usuarios de TI gestiona los conmutadores, los enrutadores y otros dispositivos del centro de datos, añádalos al destino y añada los certificados del servidor, de modo que la regla descifre el tráfico en las conexiones a sus interfaces de gestión. Si diferentes grupos de TI gestionan diferentes conjuntos de recursos del centro de datos, cree reglas estrictas diferentes en la política de seguridad y las reglas en la política de descifrado y la política de autenticación correspondientes a cada grupo.

  Para obtener acceso privilegiado a SSL:

NAME	TAGS	Source		Destination		Decrypt Options					
		ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
IT DC Management	User to DC BP	IT-Users	it-superusers	IT-Server-Access-DC	IT-Server-Management	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

  Para obtener acceso privilegiado a SSH:

NAME	TAGS	Source		Destination		Decrypt Options					
		ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
IT DC Mgmt-SSH	User to DC BP	IT-Users	it-superusers	IT-Server-Access-DC	IT-Server-Management	decrypt	ssh-proxy	DC BP Decryption	none	false	true

- Configure la inspección entrante de SSL para descifrar el tráfico permitido de grupos de usuarios empleados. En este ejemplo, se descifra tráfico de la regla análoga de permiso del grupo de usuarios de desarrollo de ingeniería.

NAME	TAGS	Source		Destination		Decrypt Options					
		ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Engg to Dev Servers	User to DC BP	Engineering-Users	api-users engg-users	Engineering-DC-Infra	Dev-Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

- Configure la inspección entrante de SSL para descifrar el tráfico permitido de contratistas, socios, clientes y terceros. En este ejemplo, se descifra tráfico de la regla análoga de permiso del grupo de usuarios de contratistas SAP.

NAME	TAGS	Source		Destination		Decrypt Options					
		ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
SAP Contractors to SAP Servers	User to DC BP	Contractors	sap-contractors	SAP-Infra	SAP DB Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

- Aplique un perfil de no descifrado para configurar la verificación del servidor para el tráfico que *decide* no descifrar debido a motivos empresariales, de reglamentación, de cumplimiento o de otro tipo, como el tráfico de finanzas, salud o gobierno. En este ejemplo, se muestra cómo excluir dos grupos de usuarios de finanzas del descifrado cuando acceden a servidores en el grupo de direcciones **Fin Servers**.

> *No aplique un perfil sin descifrado al tráfico TLSv1.3 porque la información del certificado está cifrada, por lo que el cortafuegos no puede bloquear sesiones basándose en la información del certificado.*

NAME	TAGS	Source		Destination		Decrypt Options					
		ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Finance PCI No Decrypt	User to DC BP	Finance-Users	accounting-users finance-users	Finance-DC-Infra	Fin-Servers	no-decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

Políticas de tráfico de Internet al centro de datos

Configure la política de seguridad, la política de descifrado y la política de protección de denegación de servicio (DoS) para el tráfico que va de internet al centro de datos.

- Política de seguridad de internet al centro de datos
- Política de descifrado desde internet al centro de datos
- Política de protección frente a DoS desde internet al centro de datos

STEP 1 | Cree reglas de lista de aplicaciones permitidas en la política de seguridad para el tráfico desde internet al centro de datos a fin de controlar y proteger el acceso de socios, contratistas y clientes.

Evite descargar malware de un cliente externo infectado o ubicar malware en un servidor externo desde un servidor infectado en el centro de datos. Cree reglas de permiso para aplicaciones necesarias por motivos empresariales y cree una lista dinámica externa (External Dynamic List, EDL) para bloquear direcciones IP malintencionadas. En cada regla, configure **Log at Session End (Log al finalizar sesión)** en la pestaña **Actions (Acciones)** y establezca el reenvío de logs para realizar el seguimiento y analizar los incumplimientos de la regla.

En este ejemplo, se limitan las aplicaciones y los destinos del tráfico desde internet hacia el centro de datos, y se usa la opción **Negate (Negar)** para evitar la comunicación con la EDL **Bad IPs List (Lista de IP malintencionadas)**.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Web Server Inbound	Internet to DC	universal	L3-External	~~Bad IPs List~~	any	any	Web-Server-Tier-DC	Web Servers	any	Acme	application-default	Allow		

Cree reglas similares para el tráfico desde internet hacia otros grupos de servidores (si se permite) y otras aplicaciones. Cree reglas específicas para limitar el acceso a las aplicaciones y servidores necesarios.

STEP 2 | Cree reglas en la política de descifrado para el tráfico desde internet hacia el centro de datos para descifrar el tráfico permitido.

Configure la inspección entrante de SSL (e importe los certificados del servidor de destino en el cortafuegos) para descifrar el tráfico de socios, contratistas y clientes que permiten las reglas de la política de seguridad para el tráfico desde internet hacia el centro de datos. En este ejemplo, se muestra la política de descifrado para la regla anterior de la política de seguridad.

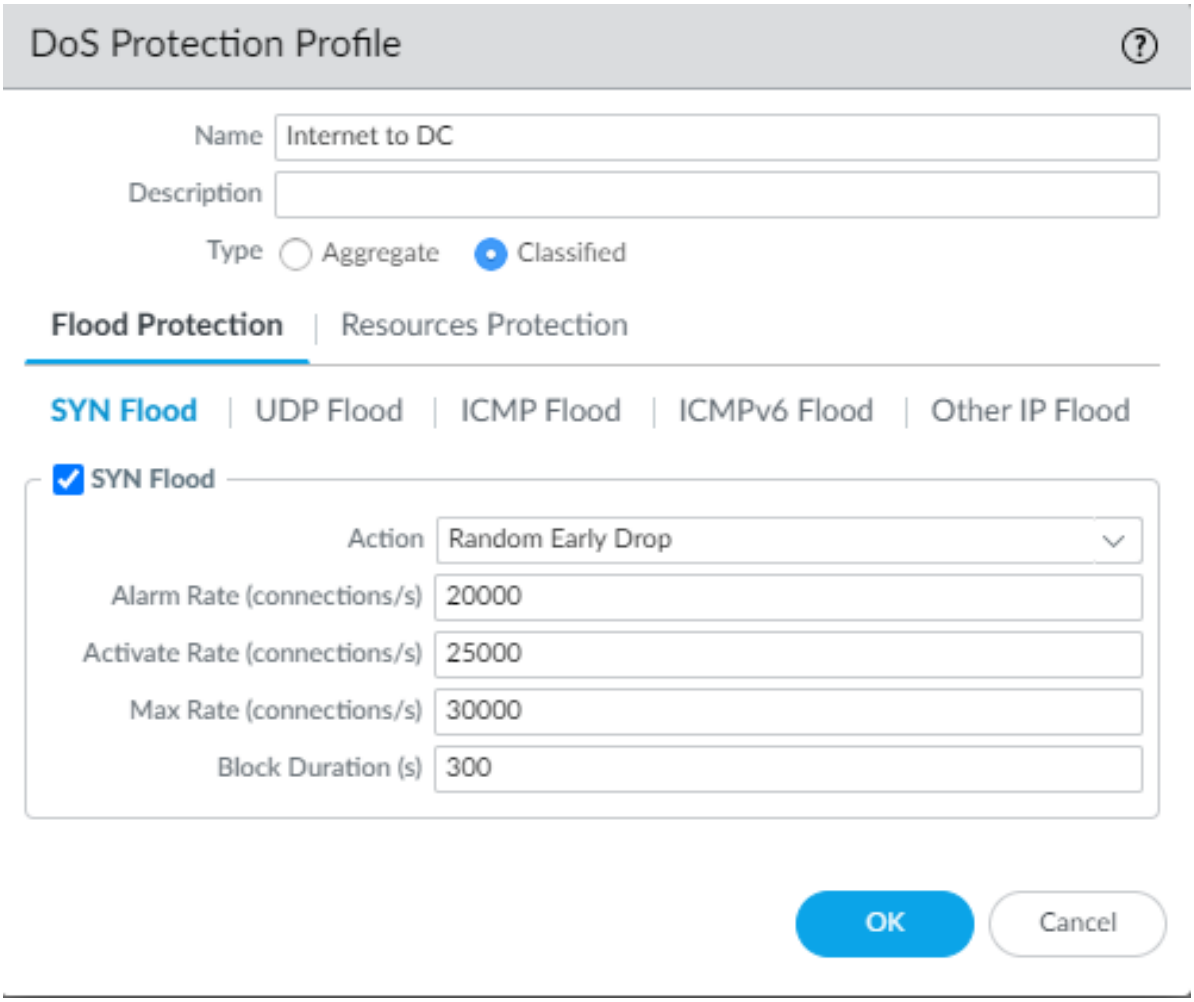
		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Internet to DC	Internet to DC BP	L3-External	any	Web-Server-Tier-DC	Web Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

Cree reglas de descifrado para que coincidan con el tráfico que permiten las reglas en la política de seguridad desde internet hacia el centro de datos.

STEP 3 | Cree reglas en la política de protección contra DoS para el tráfico desde internet hacia el centro de datos a fin de proteger a los servidores confidenciales de ataques de denegación de servicio (Denial-of-Service, DoS) limitando la cantidad de conexiones por segundo (connections-per-second, CPS) que permite el cortafuegos a los servidores para evitar un ataque de inundación SYN.

Los atacantes se dirigen al nivel de servidor web debido a que si lo inhabilitan, evitan gran parte del acceso legítimo al centro de datos. Aplique una regla en la política de protección contra DoS clasificada con un perfil de protección contra DoS que limite las CPS entrantes para evitar aumentos de tráfico que puedan afectar al rendimiento y la disponibilidad del servidor.

- Cree un perfil de protección contra DoS clasificado para proteger el nivel de servidor web y evitar ataques de inundación SYN. Los umbrales de CPS que configura dependen de la tasa máxima de CPS de referencia.



- Cree una regla en la política de protección contra DoS para especificar los servidores web que protege y aplicarles el perfil de protección contra DoS clasificado.

NAME	TAGS	Source			Destination		SERVICE	ACTION	Protection		LOG FORWARDING
		ZONE/INTERFACE	ADDRESS	USER	ZONE/INTERFACE	ADDRESS			AGGREGATE	CLASSIFIED	
DC Web Server Protection	Internet to DC BP	L3-External	~~Bad IPs List~~	any	Web-Server-Tier-DC	Web Servers	service-http service-https	protect	none	profile: Internet to DC destination-ip-only	DoS-LF

  Para protegerse de ataques internos de inundaciones SYN, cree una regla separada en la política de protección contra DoS que especifique las zonas internas como la zona de origen en lugar de **L3-External**. Separar las reglas para orígenes de ataques externos e internos permite generar informes separados que facilitan la investigación de los intentos de ataque.
- Además, configure la protección de búfer de paquetes en cada zona del centro de datos para proteger al cortafuegos de ataques de DoS de una sesión que puedan causar que se bloquee tráfico legítimo.

Políticas de tráfico del centro de datos a Internet

Configure la política de seguridad y la política de descifrado para el tráfico desde el centro de datos a Internet.

- Política de seguridad del centro de datos a Internet
- Política de descifrado del centro de datos hacia internet

STEP 1 | Cree reglas de permiso del centro de datos hacia internet para proteger las conexiones a servidores externos.

Es posible que los servidores del centro de datos obtengan las actualizaciones de software o el estado del certificado de servidores en internet. El mayor riesgo es conectarse al servidor incorrecto. Cree reglas de permiso estrictas para las actualizaciones para limitar los servidores externos con los que es posible comunicarse y las aplicaciones permitidas (en puertos predeterminados únicamente). Esto evita que los servidores infectados en el centro de datos envíen información a su origen y evita la filtración de datos con aplicaciones legítimas como FTP, HTTP o DNS en puertos no estándar. Además, use el control de **Direction (Dirección)** del perfil de bloqueo de archivos para bloquear archivos de actualización salientes, de modo que solo permita la descarga de archivos de actualización de software.

En cada regla, aplique los perfiles de seguridad recomendados y configure **Log at Session End (Log al finalizar sesión)** en la pestaña **Actions (Acciones)**.

Trabaje junto con el equipo de ingeniería y otros grupos para actualizar el software a fin de registrar y analizar sesiones de navegación web, y definir las URL a las que se conectan los desarrolladores para obtener actualizaciones.

- En estos ejemplos, se permite que los servidores de ingeniería se comuniquen con los servidores de actualización de CentOS (categoría personalizada de URL **CentOS-Update-Servers**) usando la aplicación **yum** y con los servidores de actualización de Microsoft (categoría personalizada de URL **Win-Update-Servers**) usando la aplicación **ms-update** (también debe permitir **ssl** debido a que **ms-update** depende de SSL).

			Source			Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
CentOS Update	DC to Internet BP	universal	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	yum	application-default	CentOS-Update-Servers	Allow		

			Source			Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
Windows Update	DC to Internet BP	universal	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	ms-update ssl	application-default	Win-Update-Servers	Allow		

- Permita el acceso a las actualizaciones de DNS y NTP (categoría personalizada de URL **NTP DNS Update Servers [Servidores de actualización de DNS en el NTP]**).

			Source			Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
NTP DNS Update	DC to Internet BP	universal	IT Infrastructure	DNS-NTP-Servers	any	L3-External	any	dns ntp	application-default	NTP-DNS-Update-Servers	Allow		

- Permita la conexión a un respondedor del protocolo de estado de certificado en línea (Online Certificate Status Protocol, OCSP) en internet para comprobar el estado de revocación de los certificados de autenticación y garantizar que son válidos. Cuando configure un perfil de seguridad en el cortafuegos, configure la verificación de estado de CRL como método de reserva para el OCSP en caso de que el respondedor del OCSP no se pueda comunicar.

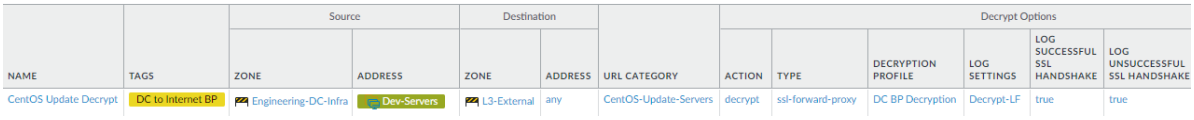
			Source			Destination						
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Cert Update	DC to Internet BP	universal	IT Infrastructure	IT-Server-Management	any	L3-External	any	ocsp	application-default	Allow		

STEP 2 | Crearan reglas en la política de descifrado para el tráfico desde el centro de datos hacia internet para descifrar el tráfico que permiten las reglas de la política de seguridad anteriores.

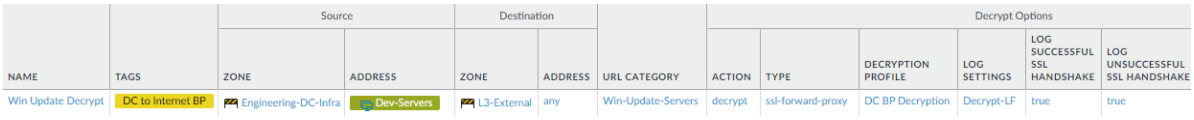
Un servidor de actualización en riesgo puede descargar malware y propagarlo a todos el proceso de actualización de software, de modo que descifrar el tráfico para obtener visibilidad es crítico. Debido a que solo las cuentas de servicio inician el tráfico de actualización y el tráfico de actualización no contiene información personal o confidencial, no hay problemas de privacidad.

No descifre tráfico que se dirige a servidores de revocación de certificados de OCSP debido a que el tráfico, por lo general, usa HTTP, de modo que no está cifrado. Además, es posible que el descifrado de proxy SSL de reenvío interrumpa el proceso de actualización debido a que el cortafuegos actúa como un proxy y reemplaza el certificado de cliente con un certificado proxy, que es posible que el respondedor de OCSP no acepte como válido.

- Descifre el tráfico entre el centro de datos y los servidores de actualización. Estos dos ejemplos descifran el tráfico de actualización de CentOS y Windows que permiten las reglas análogas en la política de seguridad del paso anterior.

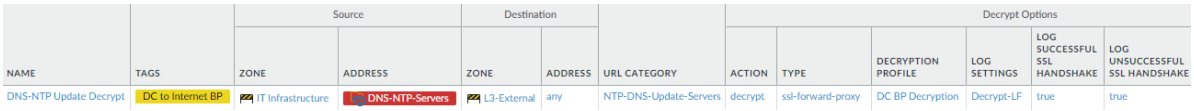


NAME	TAGS	Source ZONE	Source ADDRESS	Destination ZONE	Destination ADDRESS	URL CATEGORY	Decrypt Options ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
CentOS Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	CentOS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true



NAME	TAGS	Source ZONE	Source ADDRESS	Destination ZONE	Destination ADDRESS	URL CATEGORY	Decrypt Options ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Win Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	Win-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

- Descifre el tráfico entre los servidores del centro de datos y los servidores de actualización de NTP y DNS. En este ejemplo, se descifra el tráfico de actualización que permite la regla análoga en la política de seguridad del paso anterior.



NAME	TAGS	Source ZONE	Source ADDRESS	Destination ZONE	Destination ADDRESS	URL CATEGORY	Decrypt Options ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
DNS-NTP Update Decrypt	DC to Internet BP	IT Infrastructure	DNS-NTP-Servers	L3-External	any	NTP-DNS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

Políticas de tráfico en el centro de datos

Configure la política de seguridad y la política de descifrado para el tráfico entre los servidores del centro de datos y los niveles de aplicación.

- Política de seguridad en el centro de datos
- Política de descifrado en el centro de datos

STEP 1 | Cree reglas de aplicaciones permitidas en el centro de datos para proteger servidores de centros de datos de otros servidores de centros de datos que puedan suponer un riesgo.

Una arquitectura de aplicación habitual consiste en tres niveles de servidor: los servidores web, los servidores de la aplicación y los servidores de la base de datos. Aplique los perfiles de seguridad recomendados a la mayor parte del tráfico entre los niveles de servidor para evitar las amenazas. No aplique perfiles de seguridad a tráfico de poco valor y gran volumen como la replicación del buzón de correo electrónico y los flujos de copias de seguridad; el cortafuegos ya inspeccionó los flujos originales, de modo que dedicar ciclos de CPU en ellos no ofrece valor adicional. Cree reglas de permiso para estas aplicaciones para evitar el uso indebido. En cada regla, configure **Log at Session End (Log al finalizar sesión)** en la pestaña **Actions (Acciones)** y establezca el reenvío de logs para realizar el seguimiento y analizar los incumplimientos de la regla.

En este ejemplo, se configuran reglas que permiten el tráfico entre los niveles de servidor de la aplicación de dos aplicaciones de finanzas internas exclusivas para las que se crearon aplicaciones personalizadas: **Billing-App** y **Payment-App**.

- Permita el tráfico de la aplicación de finanzas entre el nivel de servidor web y el nivel de servidor de la aplicación.

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Web to App Server	Intra DC BP	universal	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	Billing-App Payment-App ssl web-browsing	application-default	Allow		

- Permita el tráfico de la aplicación de finanzas entre el nivel de servidor de la aplicación y el nivel de servidor de la base de datos.

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
App to DB Server	Intra DC BP	universal	App-Server-Tier-DC	Billing-App-Servers	any	DB-Server-Tier-DC	DB2-Servers	Billing-App db2 mssql-db Payment-App ssl	application-default	Allow		

STEP 2 | Cree reglas de política de descifrado en el centro de datos para descifrar el tráfico permitido en las reglas de política de seguridad anteriores.

El centro de datos es una ubicación ideal para que se oculten los atacantes debido a que muchas personas creen que el centro de datos es seguro y por tanto no lo revisan en busca de intrusos. Pero el mismo principio que se aplica al resto de las redes se aplica al centro de datos: no puede protegerse de lo que no puede ver. Descifre el tráfico cifrado del centro de datos, de modo que el cortafuegos pueda inspeccionarlo, controlar el acceso, hacer visibles las amenazas y proteger los activos valiosos.

No todo el tráfico del centro de datos está cifrado. No desperdicie recursos en el descifrado del tráfico no cifrado (texto sin formato).

- Esta regla descifra el tráfico que fluye entre el nivel del servidor web y el nivel del servidor de aplicaciones para los servidores de facturación del departamento de finanzas.

NAME	TAGS	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	Decrypt Options ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Web to App	Intra DC BP	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

- Esta regla descifra el tráfico que fluye entre el nivel del servidor de aplicaciones y el nivel del servidor de la base de datos para los servidores de facturación del departamento financiero.

NAME	TAGS	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	Decrypt Options ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
App to DB	Intra DC BP	App-Server-Tier-DC	Billing-App-Servers	any	DB-Server-Tier-DC	DB2-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

Orden de la base de reglas de la política de seguridad del centro de datos

Ordene las reglas correctamente en la base de reglas de la política de seguridad para asegurarse de que solo permite las aplicaciones y el tráfico que desea permitir y para que ninguna regla oculte otra regla.

Orden de la base de reglas de la política de seguridad del centro de datos muestra la base de reglas completa de los ejemplos anteriores (reglas de permiso y reglas de bloqueo) en el orden correcto y justifica la ubicación de cada regla.

Respeto de las prácticas recomendadas para el centro de datos tras la implementación

Después de comenzar a implementar las prácticas recomendadas para el centro de datos, supervise la red para garantizar que la seguridad y el acceso funcionen de manera adecuada, y conserve la base de reglas a medida que cambien las circunstancias.

STEP 1 | Compruebe el informe predefinido de aplicaciones [**Monitor (Supervisar)** > **Reports (Informes)** > **Application Reports (Informes de aplicaciones)** > **Applications (Aplicaciones)**] para verificar que solo se ejecutan las aplicaciones permitidas en las reglas de la política de seguridad.

Si descubre aplicaciones inesperadas, revise las reglas de la política de seguridad y vuelva a limitarlas para eliminar las aplicaciones inesperadas o incorporar aplicaciones legítimas.

STEP 2 | Registre todo el tráfico del centro de datos.

Use las herramientas detalladas de supervisión y de generación de logs, los informes predefinidos y los informes personalizados de Palo Alto Networks para capturar y supervisar la actividad de aplicaciones, usuarios, tráfico y comportamientos inesperados.

STEP 3 | Cree informes personalizados para supervisar las reglas de bloqueo, que protegen contra posibles ataques, e identifican las brechas de la política y comportamientos inesperados, de modo que pueda adaptar la base de reglas.

STEP 4 | Cree un informe personalizado para registrar el tráfico en el centro de datos que coincida con la regla de permiso intrazone-default (intrazona-predeterminada) predefinida en la parte inferior de la base de reglas, que permite todo el tráfico en la misma zona de manera predeterminada.

STEP 5 | Habilite la generación de logs y cree un informe personalizado para el tráfico en el centro de datos que coincida con la regla interzone-default (interzona-predeterminada) predefinida en la parte inferior de la base de reglas, que bloquea todo el tráfico entre zonas de manera predeterminada.

STEP 6 | Analice y responda a la opinión de los usuarios.

Las quejas del usuario acerca de la pérdida de acceso a las aplicaciones identifica brechas en la base de reglas o aplicaciones de riesgo que se usaron en la red antes de que la lista de aplicaciones permitidas evitase su uso.

STEP 7 | Compare periódicamente las mediciones de referencia que tomó durante la etapa de planificación con las mediciones actuales para evaluar el progreso, identificar cambios y descubrir áreas de mejora.

Al mismo tiempo, vuelva a considerar su objetivo futuro ideal de la red para evaluar el progreso. Si gestiona cortafuegos con Panorama, supervise el estado del cortafuegos para comparar los dispositivos con el rendimiento de referencia y entre sí para identificar las desviaciones del comportamiento normal.

STEP 8 | Permita que las reglas de aplicaciones permitidas evolucionen con el tiempo debido a que las aplicaciones evolucionan, los requisitos del usuario cambian y las actualizaciones de contenido modifican los App-ID existentes e introducen nuevos App-ID.

Realice el mantenimiento de la base de reglas recomendadas para el centro de datos y revise los App-ID nuevos y modificados antes de instalar nuevas versiones de contenido, de modo que pueda modificar la base de reglas si los cambios afectan a la política.

STEP 9 | Use las herramientas de evaluación y revisión de Palo Alto Networks para evaluar la postura de prevención actual y la adopción de las prácticas recomendadas.

STEP 10 | Consulte la política de seguridad recomendada para el centro de datos completa para obtener detalles sobre cada paso de planificación, implementación e implementación posterior, y cómo lo benefician.

Política de seguridad recomendada para el centro de datos

Los activos más valiosos de su empresa residen en su centro de datos, lo que incluye el código fuente exclusivo, la propiedad intelectual y los datos confidenciales de la empresa y el cliente. Sus clientes y empleados confían en que conservará la confidencialidad de sus datos y esperan que su centro de datos pueda accederse siempre debido a que esperan que sus datos siempre estén disponibles. Es esencial para la integridad y el éxito de su negocio que implemente una política de seguridad recomendada para el centro de datos que proteja sus datos y evite ataques exitosos.

Los siguientes métodos y recomendaciones proporcionan un modelo de planificación, diseño e implementación de una política de seguridad recomendada para el centro de datos de manera gradual y por orden de prioridad. La creación de una política de seguridad recomendada para el centro de datos puede ser intimidante si intenta implementar cada instancia de protección en cada área de la red al mismo tiempo. Sin embargo, si evalúa cuál área es la más importante y comienza a implementar la política de seguridad recomendada para el centro de datos defendiendo sus activos más valiosos en primer lugar, puede pasar gradualmente a una política de seguridad que le permita habilitar de manera segura aplicaciones, usuarios y contenido sin tomar riesgos injustificados.

La lista de verificación de la política de seguridad recomendada para el centro de datos proporciona una descripción general de la implementación previa, la implementación y la implementación posterior recomendadas, y una manera de implementar las prácticas recomendadas con mayor rapidez si no necesita explicaciones detalladas.

- ¿Qué es la política de seguridad recomendada para el centro de datos?
- ¿Por qué necesito una política de seguridad recomendada para el centro de datos?
- Metodología recomendada para el centro de datos
- ¿Cómo implemento una política de seguridad recomendada para el centro de datos?
- Evaluación del centro de datos
- Descifrado del tráfico del centro de datos
- Creación de una estrategia de segmentación de centro de datos
- Creación de perfiles de seguridad recomendados para el centros de datos
- Utilice Cortex XDR Agent para proteger los endpoints del centro de datos
- Creación de reglas de bloqueo de tráfico en el centro de datos
- Definición de la política de seguridad para el tráfico inicial desde el usuario hacia el centro de datos
- Definición de la política de seguridad para el tráfico inicial desde internet hacia el centro de datos
- Definición de la política de seguridad para el tráfico inicial desde el centro de datos hacia internet
- Definición de la política de seguridad para el tráfico inicial en el centro de datos
- Orden de la base de reglas de la política de seguridad del centro de datos
- Registro y supervisión del tráfico de centro de datos
- Mantenimiento de la base de reglas recomendadas para el centro de datos
- Uso de las herramientas de evaluación y revisión de Palo Alto Networks

¿Qué es la política de seguridad recomendada para el centro de datos?

Una política de seguridad recomendada para el centro de datos protege los datos valiosos de su empresa, protege la confidencialidad de sus clientes, socios y proveedores, protege la integridad de su red y sus operaciones de negocios, y permite garantizar la disponibilidad constante de la red. Protege contra ataques que se originan fuera o dentro de la red, en todos los vectores de ataque.

Una política de seguridad recomendada para el centro de datos protege cuatro flujos de tráfico (áreas desde donde se inician las conexiones):

1. Flujo del tráfico de usuario local hacia el centro de datos.
2. Tráfico que fluye desde internet hacia el centro de datos.
3. Tráfico que fluye desde el centro de datos hacia internet.
4. Tráfico dentro del centro de datos que fluye entre servidores o VM, también conocido como tráfico horizontal.

Una política de seguridad recomendada para el centro de datos evita que los atacantes se establezcan en el centro de datos y evita que cualquier atacante que logre filtrarse al centro de datos, filtre datos o se mueva lateralmente en la red para poner en riesgo a servidores críticos. Evita amenazas conocidas y desconocidas implementando reglas de la política de seguridad a fin de lograr los objetivos recomendados que se adaptan a sus requisitos empresariales. La política de seguridad recomendada para el centro de datos:

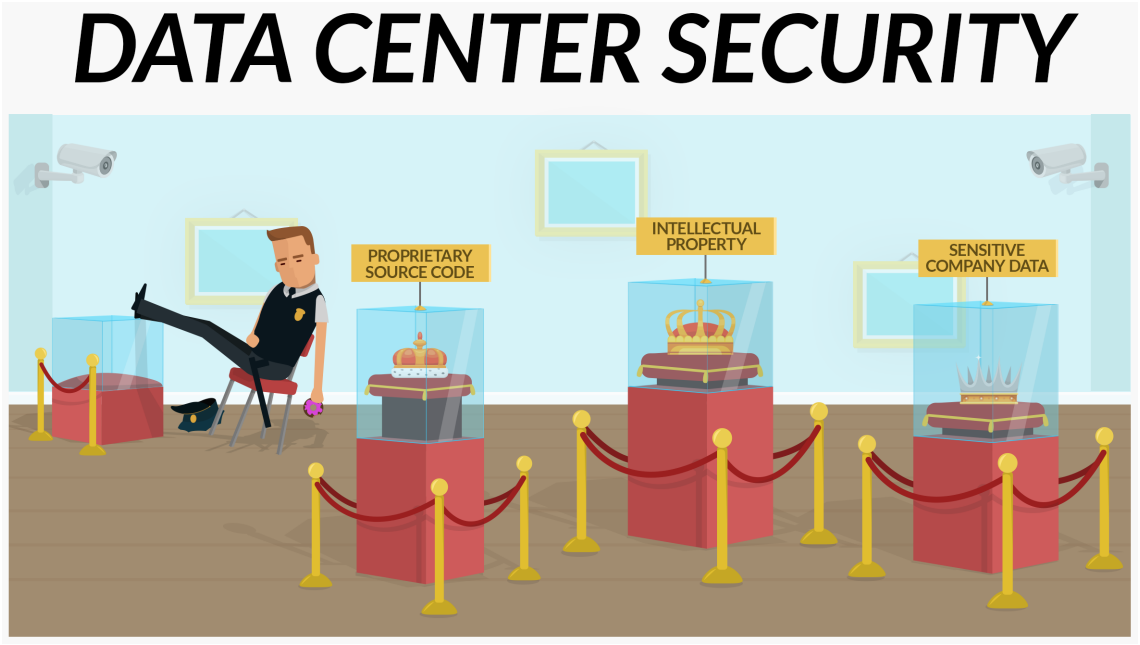
- Identifica aplicaciones independientemente del puerto, protocolo o técnica de evasión, que incluye el descifrado de tráfico cifrado.
- Identifica y controla usuarios independientemente de la dirección IP, la ubicación o el dispositivo.
- Protege frente a amenazas y vulnerabilidades conocidas y desconocidas transmitidas a través de las aplicaciones.
- Detecta comportamiento anormal que puede indicar un ataque en progreso.

Una política de seguridad recomendada para el centro de datos también captura intrusos cuando incumplen una regla de la política. Incumplir una regla detiene el ataque debido a que el incumplimiento causa que el cortafuegos de última generación detenga el acceso y garantiza el registro del incumplimiento, de modo que pueda investigar el problema y tomar las medidas adecuadas.

¿Por qué necesito una política de seguridad recomendada para el centro de datos?

Proteger la disponibilidad, la confidencialidad y la integridad de su red, de modo que pueda desarrollar su negocio de forma segura, sin interrupciones, y según la reglamentación que rige la protección de datos confidenciales, es esencial. El concepto de reforzar el exterior de la red y permitir que el interior permanezca vulnerable debido a que el interior es fiable, pero está desactualizado, no protege a la red frente a ataques internos y no prevé una situación en la que un atacante persistente, determinado y con recursos descubra una manera de establecerse dentro del perímetro. Por lo tanto, debe proteger el perímetro del centro de datos y el interior de la misma manera que protege el perímetro de la red empresarial.

Los ataques internos pueden provenir de empleados actuales o contratistas locales. El factor común de los ataques internos es que el ataque proviene de un usuario o aplicación legítimos. Los ataques externos son provocados por criminales cibernéticos, activistas hackers y atacantes patrocinados por el estado, y provienen de rutas de ataque menos obvias como sistemas de socios o proveedores en riesgo, o un antiguo empleado que conozca la red. El primer paso para un atacante externo es establecerse en la red y transformar el ataque a un ataque interno. En esencial, todas las filtraciones son ataques internos aunque se originen en el exterior, debido a que una vez que el atacante logra acceder a la red, el atacante puede recorrer la red.



Si un atacante roba las credenciales de acceso legítimas de un socio, puede acceder al centro de datos simulando ser un usuario legítimo. Entonces, desde el "interior débil y recio" de la red, el atacante puede usar los servidores internos para moverse lateralmente en la red y poner sistemas críticos en riesgo. Después de que un adversario externo acceda a la red, usted confía en que la segmentación del usuario y la red y las defensas en niveles dentro de la red protegerán sus datos, así como cuando el ataque se origina en el interior.

Desarrollar una política de seguridad recomendada permite proteger el centro de datos de ataques independientemente del origen, de manera ordenada y por orden de prioridad, y proteger los activos más valiosos primero, antes de incorporar protección adicional. Una transición gradual de una política de seguridad confiada a una política de seguridad recomendada permite garantizar la confidencialidad de

los datos, la integridad de la organización y la disponibilidad del centro de datos de manera práctica. Las siguientes recomendaciones de diseño e implementación de una política de seguridad recomendada para el centro de datos muestran como habilitar aplicaciones, usuarios y contenido de manera segura clasificando todo el tráfico, todo el tiempo con interrupciones mínimas para los usuarios finales.

Metodología recomendada para el centro de datos

Las siguientes metodologías recomendadas garantizan la detección y prevención en varias etapas del ciclo de vida del ataque.

Metodología recomendada	¿Por qué es importante?
Inspeccionar todo el tráfico para obtener visibilidad completa	Observar el tráfico de la red le permite identificar la presencia de atacantes. Inspeccione el tráfico para ver a los usuarios, las aplicaciones y el contenido que fluye hacia, en y fuera del centro de datos: ❑ Implemente cortafuegos de última generación en ubicaciones pueden inspeccionar todo el tráfico de la red. No permita que el tráfico fluya hacia el centro de datos o entre los segmentos de la red sin ubicar un cortafuegos para examinar el tráfico. ❑ Habilite el descifrado SSL en todo el tráfico que entra o sale del centro de datos, a menos que la reglamentación o las reglas de cumplimiento requieran que excluya categorías como salud, finanzas, gobierno o fuerzas armadas. Debe observar las amenazas para proteger su red contra ellas. Debido a que más del 50 por ciento del tráfico habitual de la red está cifrado y el porcentaje aumenta, si no descifra el tráfico, no podrá proteger completamente su red. ❑ Use App-ID para identificar aplicaciones y cree aplicaciones personalizadas para las aplicaciones exclusivas, de modo que el cortafuegos pueda identificar y clasificar las aplicaciones en categorías de manera adecuada, y aplicar la regla correcta de la política de seguridad. Esto es importante especialmente en el caso de las aplicaciones heredadas anteriores que, de lo contrario, se clasificarían como "web-browsing" o "unknown-tcp" en lugar de clasificarse correctamente. Si posee políticas existentes de cancelación de aplicaciones que creó únicamente para definir los tiempos de espera personalizados de una sesión en un conjunto de puertos, convierta las políticas existentes de cancelación de aplicaciones en políticas basadas en la aplicación configurando los tiempos de espera de una sesión basados en el servicio para conservar el tiempo de espera personalizado de cada aplicación y migrar la regla a una regla basada en la aplicación. Las políticas de cancelación de aplicaciones se basan en los puertos. Cuando usa políticas de cancelación de aplicaciones para conservar los tiempos de espera personalizados de una sesión en un conjunto de puertos, pierde visibilidad de la aplicación respecto a esos flujos, de modo que no sabe ni controla las aplicaciones que usan los puertos. Los tiempos de espera de una sesión basados en el servicio logran tiempos de espera personalizados y conservan la visibilidad de la aplicación. ❑ Habilite User-ID en todo el tráfico que entra o sale del centro de datos para asignar el tráfico de la aplicación y las amenazas asociadas en su contenido a los usuarios y los servicios. Ya que habilita User-ID en los segmentos de la red (zonas), debe segmentar la red para habilitar User-ID. Se recomienda segmentar la red para obtener visibilidad y reducir la superficie de ataque. ❑ Implemente GlobalProtect en modo interno como una puerta de enlace para controlar el acceso al centro de datos. GlobalProtect comprueba la información del usuario para verificar a los usuarios y alojar información a fin de garantizar que la seguridad del host esté actualizada comparando la información del host con los objetos y perfiles HIP que define. Esto garantiza que los hosts que se conecten a su red mantengan el nivel de los estándares de seguridad.

Metodología recomendada	¿Por qué es importante?
	❑ Habilite "Log at Session End" (Log al finalizar sesión) en todas las reglas de la política de seguridad. La visibilidad del tráfico permite al cortafuegos usar las tecnologías nativas App-ID, Content-ID y User-ID para unir las aplicaciones, las amenazas y el contenido a los usuarios, independientemente de la ubicación del usuario o el tipo de dispositivo, puerto, cifrado o técnica de evasión.
Reducir la superficie de ataque	La superficie de ataque consiste en todos los puntos de interacción de la red, tanto de hardware como de software, que incluye las aplicaciones, el contenido y los usuarios, además de los servidores, los conmutadores, los enrutadores, y otro equipo físico y virtual. Reducir la superficie de ataque reduce las vulnerabilidades que pueden usar los atacantes. Cuanto más reduce la superficie de ataque, más difícil es perjudicar a la red. ❑ Evalúe el centro de datos para conocer las aplicaciones, el contenido y los usuarios en la red. ❑ Use la aplicación positiva de la seguridad creando reglas basadas en la aplicación en la política de seguridad que permitan únicamente aplicaciones con usos empresariales legítimos en la red y reglas para bloquear todas las aplicaciones de alto riesgo que no cuentan con un caso de uso legítimo. ❑ Use la información de la evaluación del entorno para crear una estrategia que segmente la red en zonas en función de los requisitos empresariales, las funcionalidades habituales y los requisitos globales de la política, de modo que los recursos en cada zona requieran el mismo nivel de seguridad. En el centro de datos, segmente los niveles de las aplicaciones como las bases de datos, los servidores web, los servidores de la aplicación, los servidores de desarrollo y los servidores de producción en zonas. La segmentación le permite ver el tráfico entre los diferentes niveles de la aplicación debido a que el tráfico debe atravesar el cortafuegos cuando fluye entre zonas. La segmentación detallada le permite crear reglas en la política de seguridad que se centren en los requisitos empresariales de cada zona y brindar la protección adecuada a cada segmento. La segmentación también ayuda a detener el movimiento lateral del malware hacia y en el centro de datos debido a que la combinación de App-ID, Content-ID (prevención de amenazas) y User-ID le permite identificar el tráfico que debe poder acceder y bloquear el resto. ❑ Implemente GlobalProtect en modo interno como una puerta de enlace para controlar el acceso al centro de datos. ❑ Para reducir aún más la superficie de ataque, en las reglas de la política de seguridad que permiten el tráfico de la aplicación, aplique perfiles de bloqueo de archivos para bloquear tipos de archivo malintencionados e inseguros. Evite las filtraciones por robo de credenciales usando la política de autenticación del cortafuegos para habilitar la autenticación multifactor, de modo que incluso si los atacantes logran robar las credenciales, no puedan acceder a la red del centro de datos.
Prevenir las amenazas conocidas	Los perfiles de seguridad adjuntos a la política de seguridad permiten que las reglas analicen el tráfico en busca de amenazas conocidas como virus, spyware, vulnerabilidades de seguridad en el nivel de la aplicación, archivos malintencionados, etc. El cortafuegos aplica una acción como allow (permitir), alert (alertar), drop (eliminar), block IP (bloquear IP) o un restablecimiento de la conexión ante esas amenazas en función de la configuración del perfil de seguridad. Respete las prácticas recomendadas de actualización de contenido e instale las actualizaciones de contenido cuanto antes después de descargarlas para actualizar los perfiles de seguridad y aplicar la protección más reciente al centro de datos. Los perfiles

Metodología recomendada	¿Por qué es importante?
	de seguridad son herramientas de protección fundamentales que se pueden aplicar con facilidad a las reglas de la política de seguridad. Las listas dinámicas externas (External dynamic lists, EDL) también protegen de las amenazas conocidas. Las EDL importan listas de direcciones IP, URL o dominios malintencionados o inseguros en el cortafuegos para evitar las amenazas conocidas. Las EDL provienen de terceros de confianza, de EDL predefinidas en el cortafuegos y de EDL personalizadas que creó. Las EDL se actualizan dinámicamente en el cortafuegos sin requerir una confirmación. La prevención de las amenazas conocidas es otro motivo por el que habilitar el descifrado es importante. Si no puede ver la amenaza, no importa lo que sepa sobre ella, aún puede ser víctima debido a que no puede verla.
Prevenir amenazas desconocidas	¿Cómo se detecta una amenaza que nadie vio antes? La respuesta es reenviando todos los archivos desconocidos a WildFire para que los analice. WildFire identifica el malware desconocido o selectivo. La primera vez que un cortafuegos detecta un archivo desconocido, este reenvía el archivo a su destino interno y a la nube de WildFire para que lo analice. WildFire analiza el archivo (o un enlace en un correo electrónico) y envía un veredicto al cortafuegos en menos de cinco minutos. WildFire también incluye una firma que identifica al archivo y transforma al archivo de desconocido a conocido. Si el archivo contenía una amenaza, ahora la amenaza es conocida. Si el archivo era malintencionado, la próxima vez que llegue al cortafuegos, este lo bloqueará. Puede comprobar los veredictos en los logs de envío de WildFire (**Monitor [Supervisar]** > **Logs** > **WildFire Submissions [Envíos de WildFire]**). Configure las actualizaciones de contenido en el dispositivo WildFire para que se descarguen e instalen automáticamente, de modo que siempre tenga el soporte más reciente. Por ejemplo, el soporte para los archivos de Linux y SMB se entregó en las actualizaciones de contenido del dispositivo WildFire.

Además:

- Gestione los cortafuegos de manera centralizada con Panorama para aplicar una política uniforme en los entornos físicos y virtuales, y obtener visibilidad centralizada.
- Use la aplicación positiva de la política para permitir el tráfico que desee en la red del centro de datos y bloquear el resto.
- Cree un diseño estándar escalable que pueda replicar y aplicar de manera uniforme en los centros de datos.
- Asegúrese de que los ejecutivos, los administradores de TI y del centro de datos, y otras partes afectadas lo acepten.

Incorpore seguridad de última generación centrándose en las amenazas más probables en el negocio y la red específicos, y determine los activos más importantes que debe proteger y protéjalos primero. Formule las siguientes preguntas para permitir la priorización de protección:

1. *¿Qué convierte a nuestra empresa en lo que es?* ¿Cuáles son las propiedades que definen y diferencian a su empresa, y cuáles son los activos que las posibilitan? Los activos que se relacionan con las ventajas competitivas exclusivas de la empresa deben ser más importantes en la escala de prioridad de protección. Por ejemplo, una empresa de desarrollo de software priorizaría el código fuente o una empresa farmacéutica priorizaría las fórmulas de los medicamentos.
2. *¿Qué permite que la empresa siga funcionando?* ¿Qué sistemas y aplicaciones debe admitir la operación diaria de la empresa? Por ejemplo, el servicio de Active Directory (AD) brinda acceso a

los empleados a las aplicaciones y las estaciones de trabajo. Si pone el servicio de AD en riesgo, el atacante podrá acceder a todas las cuentas de la empresa y tendrá acceso completo a la red. Otros ejemplos incluyen una infraestructura de TI crítica, como las herramientas de gestión y los servidores de autenticación, y los servidores que alojan los datos más críticos para las operaciones del negocio.

3. *Si perdiera este activo, ¿qué sucedería?* Cuanto mayores sean las consecuencias de perder un activo, más importante deberá ser en la escala de prioridad de protección. Por ejemplo, es posible que la experiencia del usuario diferencie a una empresa de servicios, de modo que proteger esa experiencia es una prioridad. Es posible que los procesos y los equipos exclusivos diferencien a una empresa de fabricación, de modo que proteger la propiedad intelectual y los diseños exclusivos es prioridad. Cree una lista de prioridades para definir qué desea proteger primero.

Defina el estado ideal para el futuro de la red del centro de datos y trabaje en etapas para conseguirlo. Revise la definición periódicamente para tener en cuenta los cambios en el negocio, nuevos requisitos de reglamentación y jurídicos, y nuevos requisitos de seguridad.

¿Cómo implemento una política de seguridad recomendada para el centro de datos?

El flujo de trabajo de la implementación de la política de seguridad recomendada para el centro de datos consiste en obtener información sobre la red del centro de datos, sus activos y las capacidades de prevención de amenazas del cortafuegos, y crear reglas iniciales en la política de seguridad en función de la información para proteger sus activos más valiosos en primer lugar.

- Evaluación del centro de datos: identifique y priorice los activos que desea proteger, las principales amenazas para esos activos, y las aplicaciones y los usuarios con acceso sancionado.
- Descifrado del tráfico del centro de datos: no puede proteger a su red contra las amenazas que no ve. El tráfico cifrado es un método común de los atacantes para enviar amenazas.
- Creación de una estrategia de segmentación de centro de datos: segmentar el centro de datos evita que un adversario que logre establecerse en el centro de datos se mueva lateralmente hacia otras áreas.
- Creación de perfiles de seguridad recomendados para el centros de datos: las aplicaciones legítimas pueden entregar malware de mando y control, vulnerabilidades y exposiciones comunes (common vulnerabilities and exposures, CVE), descargas ocultas de contenido malintencionado, ataques de suplantación de identidad y APT. Los perfiles de seguridad recomendados protegen al tráfico permitido de amenazas conocidas y desconocidas en todos los flujos de tráfico en el centro de datos.
- Utilice Cortex XDR Agent para proteger a los endpoints del centro de datos: los cortafuegos protegen de las amenazas que atraviesan la red. Pero las amenazas que se ejecutan en el endpoint no cruzan la red, de modo que no atraviesan un cortafuegos. Instale Cortex XDR Agent en cada endpoint para protegerse de las amenazas en los endpoints.
- Cree reglas de bloqueo de tráfico en el centro de datos: bloquee direcciones IP conocidas malintencionadas, aplicaciones que los atacantes aprovechan habitualmente, aplicaciones diseñadas para evadir o saltear la seguridad, y aplicaciones que no necesita por motivos empresariales en el centro de datos.
- Defina la política de seguridad para el tráfico inicial desde el usuario hacia el centro de datos: el acceso no autorizado supone un gran riesgo para la información valiosa en el centro de datos. Dado que, por lo general, los empleados y otros usuarios en la red corporativa interna son fiables, las precauciones de seguridad suelen no ser muy estrictas. Es posible que la población de usuarios y el centro de datos se encuentre incluso en una red plana. Controle estrictamente quién puede acceder al centro de datos, los activos a los que pueden acceder los diferentes grupos de usuarios y el nivel de acceso de los diferentes grupos de usuarios a las aplicaciones.
- Defina la política de seguridad para el tráfico inicial desde internet hacia el centro de datos: proteja a los servidores del centro de datos del tráfico de internet malintencionado. Aprovechar las vulnerabilidades en el lado del servidor permite que el centro de datos sea atacado y pone a los socios en riesgo debido a que el servidor del centro de datos en riesgo puede enviar vulnerabilidades de seguridad a clientes externos.
- Defina la política de seguridad para el tráfico inicial desde el centro de datos hacia internet: el malware de mando y control que se oculta en un servidor conectado a internet infectado puede usar aplicaciones legítimas para descargar más malware. Evite que las aplicaciones usen puertos no estándar, permita únicamente transferencias de los tipos de archivos que cada aplicación puede usar de manera legítima y bloquee las categorías de URL de malware, suplantación de identidad, programas de anonimato de proxy, entre peers y otras categorías de URL potencialmente malintencionadas.
- Defina la política de seguridad para el tráfico inicial en el centro de datos (tráfico horizontal): por lo general, las amenazas provenientes del centro de datos se omiten debido a que allí no se origina tráfico y el perímetro del centro de datos se considera fiable. Sin embargo, si un atacante pone a un servidor del centro de datos en riesgo, la comunicación entre los servidores y las VM puede propagar malware. La política de seguridad recomendada evita que los atacantes se muevan lateralmente en el centro de datos y pongan a más sistemas en riesgo o filtren datos.

- Registre y supervise el tráfico de centro de datos: la generación de logs y la supervisión del tráfico permitido y bloqueado brinda información en todas las etapas de la transición y el mantenimiento de la política de seguridad recomendada para el centro de datos. Revela aplicaciones, usuarios y patrones de tráfico de la red, incluso algunos que no sabía que se encontraban allí. Esta información le permite investigar posibles problemas de seguridad.
- Realice el mantenimiento de la base de reglas recomendadas para el centro de datos: supervise la lista de aplicaciones permitidas continuamente, de modo que pueda adaptar las reglas para incorporar nuevas aplicaciones sancionadas y determinar cómo los App-ID nuevos y modificados afectan la política.

Orden de la base de reglas de la política de seguridad del centro de datos resume la base de reglas de la política de seguridad.

Evaluación del centro de datos

Para lograr un modelo de seguridad de confianza cero, debe conocer y evaluar los activos en el centro de datos, de modo que pueda establecer prioridades de protección para los activos más valiosos en primer lugar, determinar quién debe poder acceder a esos activos y comprender los principales riesgos que representan. Comprender a los usuarios que acceden a los activos, las aplicaciones permitidas y la red le permite evaluar lo que necesita y en lo que puede confiar, de modo que pueda crear una política de seguridad recomendada para el centro de datos que solo permita el acceso de usuarios y aplicaciones por motivos empresariales legítimos en la red.

1. **Realice un inventario del entorno del centro de datos:** realice un inventario de los entornos físicos y virtuales del centro de datos, que incluya los servidores, enrutadores, conmutadores, dispositivos de seguridad y otros tipos de infraestructura de red, y realice un inventario de las aplicaciones en el centro de datos (que incluya aplicaciones personalizadas desarrolladas de manera interna) y las cuentas de servicio.

   - Evalúe cada sistema según su función en la red y su importancia para el negocio a fin de establecer prioridades que fraccionen la infraestructura física y virtual que se protegerá en primer lugar. Por ejemplo, si un negocio implica la realización de transacciones con tarjetas de crédito, los servidores que gestionan transacciones de tarjetas de crédito y la ruta de comunicación del tráfico que contiene información de la tarjeta de crédito son activos extremadamente valiosos cuya protección debe ser una prioridad.
   - Examine al menos 90 días de logs de tráfico para realizar un inventario de las aplicaciones en la red del centro de datos. Cree un informe personalizado basado en la base de datos de la aplicación en el centro de datos para identificar las aplicaciones existentes en el centro de datos. Utilice el inventario de aplicaciones del centro de datos para desarrollar una lista de aplicaciones permitidas que desea para autorizar o tolerar en la red del centro de datos, como las aplicaciones personalizadas desarrolladas de manera interna.

     No es necesario que el inventario inicial de aplicaciones identifique cada aplicación debido a que mediante la supervisión de las reglas de bloqueo que configura para la base de reglas de seguridad recomendada para el centro de datos, hallará las aplicaciones que no haya identificado. Céntrese en realizar un inventario de las aplicaciones y los tipos de aplicaciones que desea permitir. Cuando termine de desarrollar la lista de aplicaciones permitidas, todas las aplicaciones que no permita explícitamente se bloquearán.

     Asigne aplicaciones a requisitos empresariales. Si una aplicación no se asigna a un requisito empresarial, evalúe si debería aceptarla en la red. Las aplicaciones que no satisfacen ninguna necesidad empresarial aparente aumentan la superficie de ataque y pueden formar parte de un conjunto de herramientas del atacante. Incluso si una aplicación innecesaria es inocente, se recomienda eliminarla, de modo que exista menos superficie que pueda aprovechar un atacante. Si varias aplicaciones realizan la misma función, por ejemplo, uso compartido de archivos o mensajería instantánea, considere configurar una o dos aplicaciones como estándar para reducir la superficie de ataque.

     Si alguna aplicación personalizada interna no usa el puerto predeterminado de la aplicación, tenga en cuenta los puertos y los servicios necesarios para admitir la aplicación personalizada. Considere volver a crear las aplicaciones personalizadas internas para usar el puerto predeterminado de la aplicación.

     Cree grupos de aplicaciones que requieran un tratamiento similar en la red, de modo que pueda aplicar la política de seguridad de manera eficiente a los grupos de aplicaciones, en lugar de hacerlo a aplicaciones individuales. Los grupos de aplicaciones facilitan el diseño y la implementación de una política de seguridad debido a que puede aplicar la política a todas las aplicaciones en un grupo a la

vez, cambiar la política de todo el grupo, añadir aplicaciones nuevas al grupo para aplicar la política del grupo a las aplicaciones nuevas y reusar un grupo de aplicaciones en varias reglas de la política de seguridad. Por ejemplo, un grupo de aplicaciones diseñado para las aplicaciones de almacenamiento del centro de datos puede incluir aplicaciones como crashplan, ms-ds-smb y NFS.

- Realice un inventario de las cuentas de servicio que usan las aplicaciones para comunicarse entre servidores y dentro de los servidores en el centro de datos. Se recomienda usar una cuenta de servicio para cada función, en lugar de una cuenta de servicio para varias funciones. Esto limita el acceso a la cuenta de servicio y facilita la comprensión de cómo se usa la cuenta de servicio si un sistema está en riesgo. También se recomienda identificar las cuentas de servicio que se codifican de forma rígida en la aplicación, de modo que pueda crear firmas de IPS para ellas y supervisar el uso de las cuentas.

2. **Caracterice el tráfico del centro de datos:** caracterice y asigne el tráfico del centro de datos para comprender cómo fluyen los datos en la red y entre usuarios y recursos. Involucre a un equipo interdisciplinario que incluya arquitectos de aplicaciones, de redes y empresariales, y representantes del negocio. Caracterizar los flujos de tráfico le brinda información sobre los orígenes y los destinos del tráfico de la red, los patrones y las cargas habituales del tráfico, y le permite comprender el tráfico de la red y establecer una prioridad de protección para el tráfico. Use los widgets del centro de control de aplicaciones, las funciones de supervisión de estado del cortafuegos de Panorama y otros métodos para comprender los patrones habituales (de referencia) de tráfico, lo que le permite identificar patrones de tráfico anormales que puedan indicar un ataque.
3. **Acceda a la segmentación del centro de datos:** segmente los niveles de servidor del centro de datos, de modo que la comunicación entre los diferentes niveles de servidor deba pasar por el cortafuegos de última generación para que se descifre, examine y proteja con la política de seguridad recomendada, y que la comunicación entre la población de usuarios e internet pase por un cortafuegos de última generación. Fuera del centro de datos, comprenda qué zonas *pueden* comunicarse con cada zona en el centro de datos y determine qué zonas *deben* poder comunicarse con cada zona en el centro de datos.
4. **Acceda a la segmentación de la población de usuarios y determine quién debe poder al centro de datos:** asigne usuarios a grupos para segmentar la población de usuarios, de modo que pueda controlar con mayor facilidad el acceso a los sistemas confidenciales. Por ejemplo, los usuarios en el grupo de gestión de productos no deben poder acceder a los sistemas de finanzas o recursos humanos. En Active Directory (o el sistema que use), cree grupos de usuarios detallados basados en el nivel de acceso que requieren los usuarios por motivos empresariales legítimos, de modo que pueda controlar el acceso a los sistemas y las aplicaciones. Esto incluye los diferentes grupos de empleados, además de los diferentes contratistas, socios, clientes y grupos de proveedores, agrupados por nivel de acceso necesario.

   Reduzca la superficie de ataque creando grupos de usuarios según los requisitos de acceso, en lugar de la funcionalidad, y conceda únicamente el nivel adecuado de acceso a la aplicación a cada grupo. En un área funcional como la de marketing o la de los contratistas, cree varios grupos de usuarios vinculados a determinados requisitos de acceso a aplicaciones.
5. **Supervise continuamente la red del centro de datos:** registre y supervise el tráfico del centro de datos para revelar brechas en la política de seguridad recomendada para el centro de datos, exponer patrones de tráfico anormales o intentos de acceso inesperados que puedan indicar un ataque, o diagnosticar los problemas de la aplicación.

Un método útil para evaluar activos es agrupándolos. Identifique los activos más valiosos que deben protegerse primero e identifique los activos que puede repetir después de proteger a esos activos. Establezca una prioridad de protección para los activos en cada categoría. Organice los activos de la manera más razonable para el negocio específico. La siguiente tabla muestra algunas posibilidades, pero no está completo. Además, considere los requisitos de cumplimiento legal de proteger datos como contraseñas, información personal e información financiera cuando establezca una prioridad de protección.

Table 1: Ejemplos de categorías de activos

Activos más valiosos	Otros activos valiosos	Activos restantes (repetir)
• Patentes • Código fuente • Datos confidenciales como los diseños de los productos, las fórmulas de los medicamentos o los datos de usuarios. • Algoritmos exclusivos • Certificados de firma de código y PKI (son clave para su cifrado) • Servidor de dominio de AD (si pierde AD, un atacante podrá crear credenciales que brindan acceso ilimitado a la red) • Otros activos muy valorados que diferencian a su negocio del resto	• Infraestructura de TI crítica como enrutadores o interfaces del cortafuegos • Servicios de autenticación • EMAIL • VPN, en especial, para empresas muy distribuidas • Aplicaciones empresariales críticas • Servidores de uso compartido de archivos • Bases de datos	• Equipo de laboratorio de red • Sistemas de gestión de TI • Otros activos

La prioridad de los activos es única para cada negocio. En una empresa de servicios, es posible que la experiencia del usuario diferencie al negocio de otros, de modo que los activos más valiosos serán activos que garanticen una mejor experiencia del usuario. En una empresa de fabricación, es posible que los activos más valiosos sean los procesos y los diseños de equipos exclusivos. Considerar las consecuencias de perder un activo es una buena manera de descubrir cuáles debe proteger en primer lugar.

Descifrado del tráfico del centro de datos

No es posible proteger la red de amenazas que no se puede ver o inspeccionar. El descifrado del tráfico para exponer el malware es fundamental porque la mayor parte del tráfico de una red típica viene cifrada y el volumen va en aumento. Un porcentaje cada vez mayor de campañas de malware que ocultan intrusiones en la red, instalan malware de comando y control y extraen datos, también utilizan el cifrado.

Para exponer a las aplicaciones y las amenazas cifradas, ubique cortafuegos físicos o virtuales de última generación, de modo que visualicen todo el tráfico en el centro de datos. Descifre todo el tráfico posible, en especial, las categorías de tráfico de alto riesgo, el tráfico destinado a servidores críticos y el tráfico crítico para el negocio. El descifrado de tráfico permite identificar ese tráfico correctamente, de modo que el cortafuegos pueda aplicar antivirus, protección frente a vulnerabilidades, WildFire y otras protecciones frente a amenazas adecuadamente.

Para aplicar el descifrado al tráfico, cree perfiles de descifrado que especifiquen cómo tratar tráfico TLS y SSH, y el tráfico que decide no descifrar o que no se puede descifrar. Los perfiles de descifradodefinen los protocolos, algoritmos, modos y las características de la sesión del tráfico permitidos. Aplique perfiles de descifrados a las reglas de la política de descifrado, que especifican el tráfico al que el cortafuegos aplica los perfiles de descifrado.

El cortafuegos admite dos tipos de descifrado SSL/TLS y descifrado SSH:

- Proxy de reenvío SSL (tráfico saliente)
- Inspección de entrada SSL (tráfico de entrada)
- Proxy SSH (generalmente para el acceso seguro para administradores que administran dispositivos de red)

En el centro de datos, descifre cuanto tráfico horizontal sea posible. Si las consideraciones de rendimiento causadas por un establecimiento erróneo del tamaño evitan que descifre todo el tráfico, establezca una prioridad para los servidores más críticos, las categorías de tráfico con mayor riesgo y los segmentos y las subredes de IP menos fiables, y descifre cuanto tráfico sea posible garantizando un rendimiento aceptable. Las principales preguntas con las siguientes: "¿Qué sucede si el servidor está en riesgo?", "¿Cuánto riesgo representa cada categoría de tráfico?" y "¿Cuánto riesgo estoy dispuesto a aceptar en cuando al nivel de rendimiento que deseo lograr en el centro de datos?"

En el tráfico que fluye desde el centro de datos hacia internet, descifre todo, a excepción del tráfico que requiere una excepción. La visibilidad que el descifrado proporciona es especialmente importante debido a que no desea que los servidores en el centro de datos se conecten a sitios malintencionados, transfieran archivos malintencionados o estén vulnerables a descargas de malware.

Cuando planifique la política de descifrado, considere las reglas de cumplimiento de seguridad de la empresa y las ubicaciones. En el tráfico desde los usuarios hacia el centro de datos, a pesar de que es posible que una política de descifrado estricta provoque inicialmente algunos reclamos, esos reclamos pueden indicarle sitios web no sancionados o no deseados que están bloqueados debido a que sus algoritmos son débiles o tienen problemas relacionados a los certificados. Use las reclamaciones como una herramienta para comprender mejor el tráfico de su red.

Además, habilite el Registro de descifrado en las políticas de descifrado y, si los recursos lo permiten, registre los protocolos de enlace SSL que se han realizado con éxito o que han fallado. Aproveche todas las Herramientas de resolución de problemas y supervisión de descifrado para examinar su implementación y ajustar sus políticas y perfiles.

El descifrado de tráfico consume recursos del cortafuegos. La cantidad de tráfico que descifre variará según el centro de datos. Cuando ajuste el tamaño de la implementación del cortafuegos para garantizar un rendimiento aceptable y admitir el descifrado, tenga en cuenta la cantidad de tráfico que planea descifrar (algunas aplicaciones deben descifrarse, mientras que otras aplicaciones no están cifradas y no es necesario descifrarlas), el

cifrado de descifrado (los cifrados más sólidos y complejos requieren mayor capacidad de procesamiento durante el descifrado), el tamaño de las claves (las claves de mayor tamaño consumen más recursos de descifrado), el tipo de intercambio de claves (por ejemplo, los intercambios de claves RSA consumen más recursos de procesamiento que las claves PFS) y la capacidad de los cortafuegos. Trabaje con el equipo de ventas y los representantes de Palo Alto Networks para ajustar el tamaño de la implementación de cortafuegos de manera adecuada para su red específica, de modo que pueda descifrar el tráfico y exponer las amenazas.

Las empresas con negocios, como los bancos, que requieren una seguridad extremadamente sólida para las claves privadas puede usar un módulo de seguridad de hardware (Hardware Security Module, HSM) externo para proteger y gestionar la clave privada de la empresa, en lugar de almacenarla en el cortafuegos.

- Creación de perfiles de descifrado recomendados para el centro de datos
- Exclusión del tráfico inadecuado del descifrado del centro de datos

Creación de perfiles de descifrado recomendados para el centro de datos

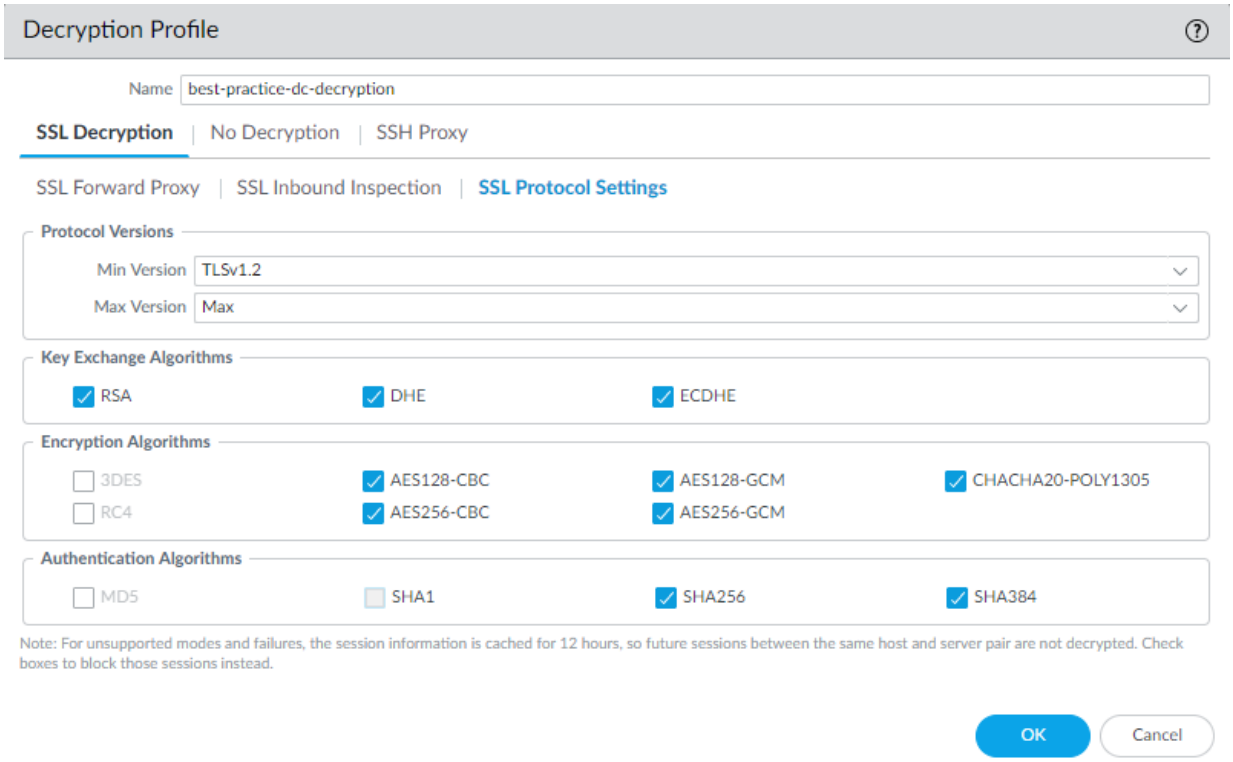
Los perfiles de descifrado especifican cómo el cortafuegos comprueba el tráfico descifrado y el tráfico que puede o decide no descifrar. El cortafuegos comprueba los protocolos, los certificados de servidor, las características de la sesión y las cifras (algoritmos de intercambio de claves, algoritmos de cifrado y algoritmos de autenticación). Aplique los perfiles de descifrado [**Objects (Objetos)** > **Decryption Profile (Perfil de descifrado)**] a las reglas en la política de descifrado [**Policies (Políticas)** > **Decryption (Descifrado)**]. Las reglas en la política de descifrado definen el tráfico a comprobar usando el origen, el destino, la categoría de servicio y la categoría de URL como criterio de coincidencia, de modo que tenga control detallado sobre el tráfico al que aplica un perfil de descifrado. También debe configurar el registro de descifrado y el reenvío de log en la regla de política.

Para descifrar el tráfico saliente, el cortafuegos actúa como un dispositivo proxy de reenvío entre el cliente interno y el servidor externo. Para inspeccionar el tráfico entrante, el cortafuegos realiza una copia del tráfico de la sesión entrante, y descifra e inspecciona la copia.

STEP 1 | Configure el cortafuegos para que realice comprobaciones de CRL/OCSP para garantizar que los certificados que se presentan durante el descifrado SSL sean válidos.

STEP 2 | Configure los ajustes en **SSL Decryption (Descifrado SSL)** > **SSL Protocol Settings (Ajustes de protocolo SSL)** para bloquear versiones SSL/TLS vulnerables como TLSv1.0, TLSv1.1 y SSLv3, evitar algoritmos de cifrado débiles como RC4 y 3DES y algoritmos de autenticación débiles como MD5 y SHA1.

Los ajustes del protocolo SSL se aplican a todo el tráfico descifrado.



Establezca el protocolo **Min Version (Versión mínima)** en **TLSv1.2** y el protocolo **Max Version (Versión máxima)** en **Max (Máximo)** para bloquear protocolos débiles. Utilice el protocolo TLS más fuerte disponible. Cree políticas y perfiles de descifrado independientes para maximizar la seguridad. Por ejemplo, si los sitios heredados que necesita con fines comerciales solo admiten protocolos más débiles, cree un perfil de descifrado diferente para permitir estos protocolos y aplíquelo en una política de descifrado solo en los sitios que no son compatibles con al menos TLSv1.2. Esto también se aplica a los sitios comerciales necesarios que no admiten algoritmos fuertes y para diferentes categorías de URL para ajustar la seguridad frente al rendimiento.

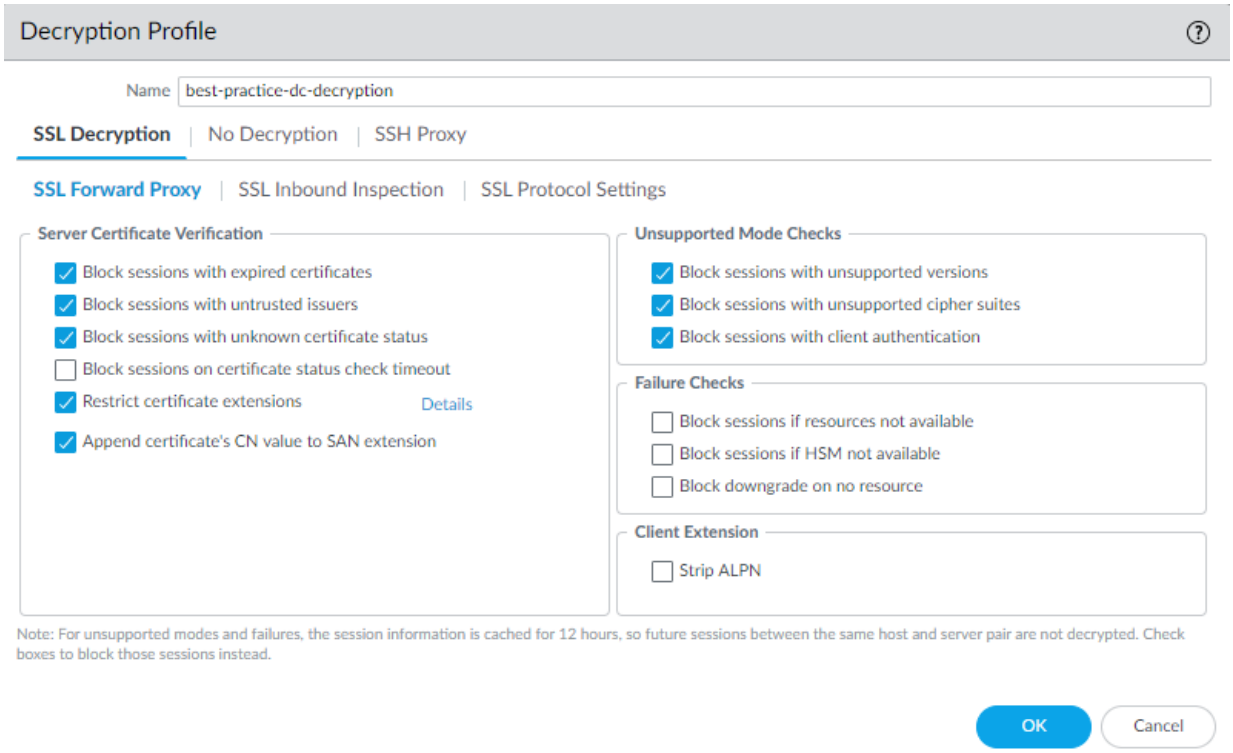
Si el sitio no tiene una aplicación comercial legítima, no debilite su seguridad para admitir este sitio; los protocolos y cifrados débiles contienen vulnerabilidades conocidas que los atacantes pueden aprovechar. Si el sitio pertenece a una categoría de sitios que no necesita con fines comerciales, use el filtrado de URL para bloquear el acceso a la categoría completa. No admita protocolos débiles o cifrado débil, o algoritmos de autenticación débiles a menos que deba hacerlo para permitir sitios heredados importantes.

Configure la **Max Version (Versión máxima)** en **Max (Máxima)** en lugar de configurarla en una versión determinada, de modo que a medida que los protocolos mejoren, el cortafuegos admita automáticamente los mejores protocolos más nuevos. Tanto si adjunta un perfil de descifrado a una regla de política de descifrado que rige el tráfico de entrada (Inspección de entrada SSL) o el de salida (proxy SSL de reenvío), evite los algoritmos débiles.

Muchas aplicaciones móviles utilizan certificados anclados. Debido a que TLSv1.3 cifra la información del certificado, el cortafuegos no puede añadir automáticamente estas aplicaciones móviles a la Lista de exclusión de descifrado SSL. Para estas aplicaciones, asegúrese de que la Versión máxima del perfil de descifrado esté configurada en TLSv1.2 o aplique una política de No descifrado al tráfico.

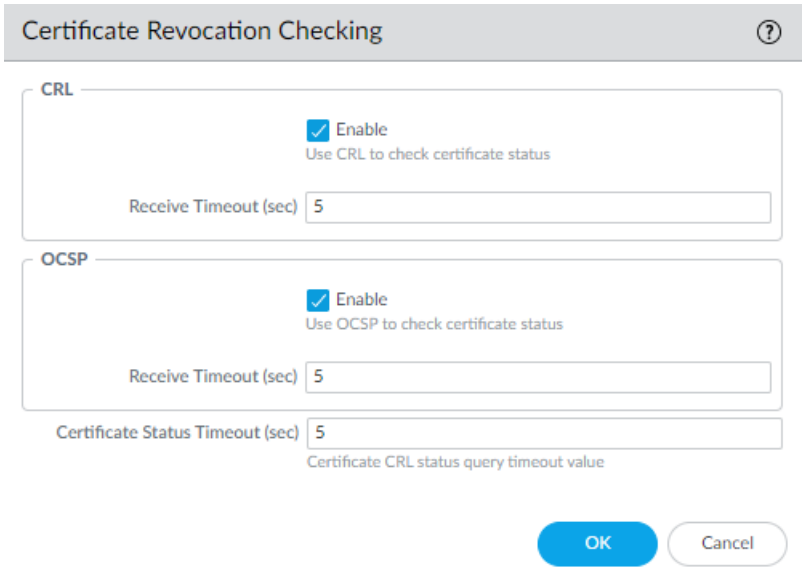
STEP 3 | Configure los ajustes en **SSL Decryption (Descifrado SSL)** > **SSL Forward Proxy (Proxy de reenvío SSL)** para el tráfico saliente a fin de bloquear las excepciones durante la negociación TLS y bloquear las sesiones que no puedan descifrarse.

En algunos casos, los ajustes recomendados dependen de las reglas de cumplimiento de seguridad de su empresa. Aplique el perfil de descifrado de proxy de reenvío SSL a las reglas de la política de seguridad que controlan el tráfico saliente.



Bloquee las excepciones durante la negociación de TLS y bloquee las sesiones que no se puedan descifrar.

- **Verificación de certificados de servidor:** seleccionar la casilla de verificación **Block sessions on certificate status check timeout (Bloquear sesión al agotar el tiempo de espera de comprobación de estado de certificado)** depende de la postura de cumplimiento de seguridad de la empresa debido a que se trata de una compensación entre una seguridad más estricta y una mejor experiencia del usuario. La verificación de estado del certificado examina la lista de revocación de certificados (Certificate Revocation List, CRL) en un servidor de revocación o usa un Protocolo de estado de certificado en línea (Online Certificate Status Protocol, OCSP) para definir si la CA emisora revocó el certificado y no se debe confiar en él. Sin embargo, los servidores de revocación pueden tardar en responder, lo que puede provocar que se agote el tiempo de espera de la sesión y el cortafuegos bloquee la sesión aunque el certificado sea válido. Si selecciona **Block sessions on certificate status check timeout (Bloquear sesión al agotar el tiempo de espera de comprobación de estado de certificado)** y el servidor de revocación responde lentamente, puede usar **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** > **Decryption Settings (Ajustes de descifrado)** y hacer clic en **Certificate Revocation Checking (Comprobación de revocación de certificados)** para cambiar el valor predeterminado de tiempo de espera de cinco segundos a otro valor.



Habilite la comprobación de revocación de certificados de CRL y de OCSP porque los certificados de servidor pueden contener URL de CRL en la extensión del Punto de distribución de CRL (CRL Distribution Point, CDP) o URL de OCSP en la extensión de certificado de Acceso a la información de la entidad (Authority Information Access, AIA).

A pesar de que se recomienda usar un certificado adecuado, algunos certificados dejan el campo Nombre alternativo del sujeto (Subject Alternate Name, SAN) vacío, lo que puede provocar que los cortafuegos bloqueen estos certificados. Seleccione **Append certificate's CN value to SAN extension (Anexar valor del CN del certificado a la extensión SAN)** para copiar automáticamente el nombre del certificado en el campo SAN si el campo SAN está vacío, de modo que si hace negocios con sitios que no completan el campo SAN del certificado, puede aceptar sus certificados. De lo contrario, los sitios deben regenerar sus certificados para respetar la práctica adecuada y completar el campo SAN.

Bloquee todas las excepciones de verificación de certificados de servidor.

- **Comprobaciones de modo no admitidas:** si no bloquea sesiones con versiones y conjuntos de cifrado no admitidos, los usuarios recibirán un mensaje de advertencia en el que podrán hacer clic y acceder al sitio web inseguro. El motivo de configurar ajustes de protocolo SSL estrictos es bloquear y protegerse de los servidores que usan estas versiones y algoritmos de protocolo débiles (inseguros). Además, bloquear las sesiones con comprobaciones de modo no admitidas protege contra puertas traseras malintencionadas y otras amenazas que usan cifrado personalizado y no estándar para ofuscar sus actividades.

  Bloquear sesiones con autenticación de cliente le permite decidir si desea permitir o bloquear las sesiones que usan autenticación de cliente. A pesar de que la autenticación de servidor es la única autenticación que se puede usar para establecer una sesión, algunos sitios usan autenticación mutua, en la cual el servidor y el cliente se autentican para establecer una sesión. La autenticación de cliente con un certificado digital X.509 es similar a la autenticación de servidor dado que ambos métodos usan un certificado digital emitido por una autoridad de certificado de confianza para autenticar una sesión. El certificado de cliente actúa como un identificador digital para el cliente, reside en el dispositivo cliente y no puede transferirse a otros dispositivos. Sin embargo, la autenticación de cliente evita que el cortafuegos descifre la sesión debido a que el cortafuegos requiere los certificados de cliente y de servidor para realizar el descifrado bidireccional, pero el cortafuegos solo conoce el certificado de servidor. Esto interrumpe el descifrado para las sesiones con autenticación de cliente.

  Si no habilita **sesiones de bloqueo con autenticación de cliente**, cuando el cortafuegos intenta descifrar una sesión que usa la autenticación de cliente, permite la sesión y añade una entrada en su caché de exclusión de descifrado local que contiene la dirección IP/URL del servidor, la aplicación

y el perfil de descifrado. Las entradas permanecen en la caché durante 12 horas y luego caducan. Si el mismo usuario o uno diferente intenta acceder al servidor en un período de 12 horas con la autenticación de cliente, el cortafuegos coteja la sesión con la entrada de caché de exclusión de descifrado, no intenta descifrar el tráfico y permite la sesión cifrada.

Si la caché de exclusión se llena, el cortafuegos depura las entradas más antiguas a medida que llegan las nuevas. Si cambia el perfil o la política de descifrado, el cortafuegos renueva la caché de exclusión porque si cambia la política o el perfil, puede cambiar el resultado de clasificación de la sesión.

Si habilita **Bloquear sesiones con autenticación de cliente**, el cortafuegos bloquea las sesiones que usan autenticación de cliente, a excepción de las sesiones de sitios en la lista de exclusión de descifrado SSL (**Device [Dispositivo]** > **Certificate Management [Gestión de dispositivos]** > **SSL Decryption Exclusion [Exclusión de descifrado SSL]**).

Es posible que deba permitir el tráfico en su red de otros sitios que usen la autenticación de cliente además de los sitios predefinidos en la lista de exclusión de descifrado SSL. Cree un perfil de descifrado que permita las sesiones con autenticación de cliente. Añádalo a la regla de política de descifrado que se aplica solo a los servidores que tienen la aplicación. Para aumentar aún más la seguridad, puede requerir la autenticación multifactor para completar el proceso de inicio de sesión del usuario.

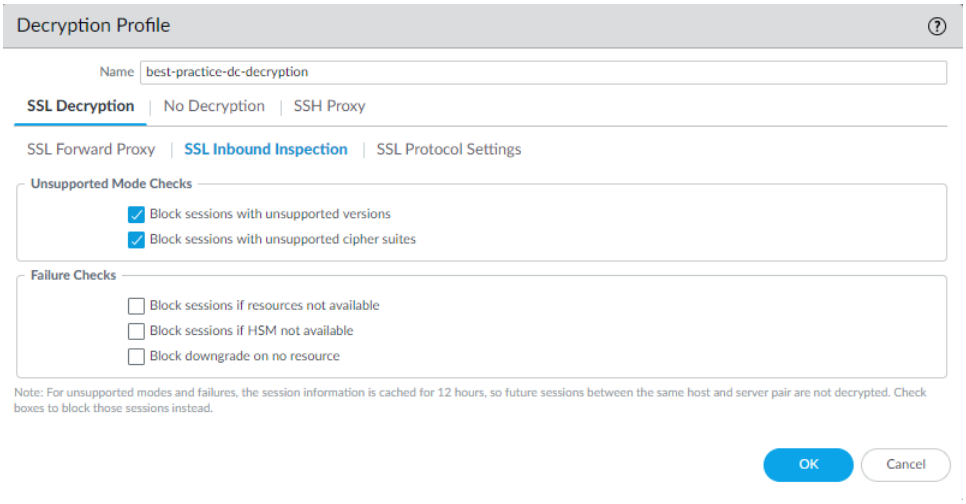
En el resto del tráfico, aplique el perfil de descifrado que bloquea sesiones con autenticación de cliente.

- **Comprobaciones de fallos:** si no selecciona **Block sessions if resources not available (Bloquear sesiones si los recursos no están disponibles)**, el riesgo es que la falta de recursos de procesamiento puede permitir conexiones potencialmente peligrosas. Si bloquea sesiones con recursos no disponibles, es posible que afecte la experiencia del usuario. Implementar o no las comprobaciones de fallas depende de la posición de cumplimiento de seguridad de su empresa y de la importancia que su empresa le dé a la experiencia de usuario, en comparación con una seguridad más estricta.

  Si usa un módulo de seguridad de hardware (Hardware Security Module, HSM) para almacenar las claves privadas, seleccionar **Block sessions if HSM not available (Bloquear sesiones si el HSM no está disponible)** depende de las reglas de cumplimiento relacionadas con el origen de las claves privadas y cómo desea manejar el tráfico cifrado si el HSM no está disponible. Por ejemplo, si su empresa exige el uso de un HSM para la firma de claves privadas, entonces, bloquea las sesiones si el HSM no está disponible. Sin embargo, si su empresa es menos estricta en este aspecto, entonces puede considerar no bloquear sesiones si el HSM no está disponible. (Si el HSM no está disponible, el cortafuegos puede procesar el descifrado de los sitios para los cuales tiene almacenado en caché la respuesta del HSM, pero no para otros sitios). La acción recomendada en este caso depende de las políticas de su empresa. Si el HSM es crítico para su empresa, ejecútelo en el par de alta disponibilidad (high-availability, HA) (PAN-OS 8.0 admite dos miembros en un par de HA de HSM).
- **Bloquear el cambio a una versión anterior sin recurso**: con esta opción, se evita que el cortafuegos cambie de una versión TLSv1.3 a TLSv1.2 si este no tiene recursos de procesamiento TLSv1.3 disponibles. Si bloquea el cambio a una versión anterior, cuando el cortafuegos se quede sin recursos TLSv1.3, descartará el tráfico que usa TLSv1.3 en lugar de degradarlo a TLSv1.2. Si no bloquea el cambio a una versión anterior, cuando el cortafuegos se quede sin recursos TLSv1.3, se degradará a TLSv1.2. Sin embargo, bloquear el cambio a una versión anterior cuando los recursos no están disponibles puede afectar la experiencia del usuario porque los sitios a los que acceden los usuarios con normalidad, por el momento no están disponibles. Implementar o no esta comprobación de fallos depende de la posición de cumplimiento de seguridad de su empresa y de la importancia de la experiencia de usuario, en comparación con una seguridad más estricta. Es posible que desee crear una política y un perfil de descifrado independientes para regular el descifrado del tráfico sensible para el que no desee degradar la versión TLS.

STEP 4 | Configure los ajustes de **SSL Decryption (Descifrado SSL)** > **SSL Inbound Inspection (Inspección entrante de SSL)** para inspeccionar el tráfico desde un cliente externo hacia los servidores internos y bloquear las sesiones sospechosas.

Aplique el perfil de descifrado de inspección entrante de SSL a las reglas de la política de seguridad que controlan el tráfico entrante.



- **Comprobaciones de modo no admitidas:** el cortafuegos no puede descifrar las versiones y los cifrados de sesiones que el cortafuegos no admite. Para evitar que los atacantes usen versiones y cifrados no admitidos para acceder sigilosamente a la red, bloquee las versiones y los conjuntos de cifrado de las sesiones que el cortafuegos no admite. Además, bloquear las sesiones con comprobaciones de modo no admitidas protege contra puertas traseras malintencionadas y otras amenazas que usan cifrado personalizado y no estándar para ofuscar sus actividades.

  En el servidor, habilite únicamente el cifrado que admite en el cortafuegos. Garantizar la compatibilidad simplifica la negociación entre el cliente y el servidor.
- **Comprobaciones de fallos:** si no selecciona **Block sessions if resources not available (Bloquear sesiones si los recursos no están disponibles)**, el riesgo es que la falta de recursos de procesamiento puede permitir conexiones potencialmente peligrosas. Si bloquea sesiones con recursos no disponibles, es posible que afecte la experiencia del usuario. Implementar o no las comprobaciones de fallas depende de la posición de cumplimiento de seguridad de su empresa y de la importancia que su empresa le dé a la experiencia de usuario, en comparación con una seguridad más estricta.

  Si usa un módulo de seguridad de hardware (Hardware Security Module, HSM) para almacenar las claves privadas, seleccionar **Block sessions if HSM not available (Bloquear sesiones si el HSM no está disponible)** depende de las reglas de cumplimiento relacionadas con el origen de las claves privadas y cómo desea manejar el tráfico cifrado si el HSM no está disponible. Por ejemplo, si su empresa exige el uso de un HSM para la firma de claves privadas, entonces, bloquea las sesiones si el HSM no está disponible. Sin embargo, si su empresa es menos estricta en este aspecto, entonces puede considerar no bloquear sesiones si el HSM no está disponible. (Si el HSM no está disponible, el cortafuegos puede procesar el descifrado de los sitios para los cuales tiene almacenado en caché la respuesta del HSM, pero no para otros sitios). La acción recomendada en este caso depende de las políticas de su empresa. Si el HSM es crítico para su empresa, ejecútelo en el par de alta disponibilidad (high-availability, HA) (PAN-OS 8.0 admite dos miembros en un par de HA de HSM).
- **Bloquear el cambio a una versión anterior sin recurso**: con esta opción, se evita que el cortafuegos cambie de una versión TLSv1.3 a TLSv1.2 si este no tiene recursos de procesamiento TLSv1.3 disponibles. Si bloquea el cambio a una versión anterior, cuando el cortafuegos se quede sin recursos TLSv1.3, descartará el tráfico que usa TLSv1.3 en lugar de degradarlo a TLSv1.2. Si no bloquea el cambio a una versión anterior, cuando el cortafuegos se quede sin recursos TLSv1.3, se degradará a TLSv1.2. Sin embargo, bloquear el cambio a una versión anterior cuando los recursos no están disponibles puede afectar la experiencia del usuario porque los sitios a los que acceden los usuarios con normalidad, por el momento no están disponibles. Implementar o no esta comprobación de fallos depende de la posición de cumplimiento de seguridad de su empresa y de la importancia de la

experiencia de usuario, en comparación con una seguridad más estricta. Es posible que desee crear una política y un perfil de descifrado independientes para regular el descifrado del tráfico sensible para el que no desee degradar la versión TLS.

STEP 5 | Para el tráfico SSH, configure los ajustes del perfil de descifrado de proxy SSH.

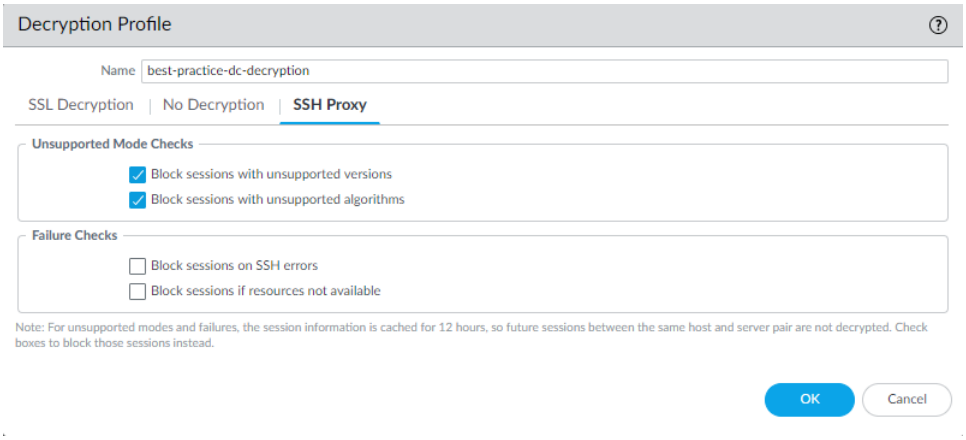
El descifrado SSH permite el tráfico SSH que se enruta habitualmente y bloquea el tráfico de tunelización SSH (reenvío de puertos SSH), pero no realiza la inspección del contenido o las amenazas en el tráfico SSH. Las sesiones de canalización SSH pueden canalizar paquetes de Windows X11 y TCP. Una conexión SSH puede contener varios canales. Cuando aplica un perfil de descifrado SSH al tráfico, en cada canal de la conexión, el cortafuegos examina el App-ID del tráfico e identifica el tipo de canal. El tipo de canal puede ser uno de los siguientes:

- sesión
- X11
- forwarded-tcpip
- direct-tcpip

Cuando el tipo de canal es sesión, el cortafuegos identifica el tráfico como tráfico SSH permitido como FTP o SCP. Cuando el tipo de canal es X11, forwarded-tcpip, or direct-tcpip, el cortafuegos identifica el tráfico como tráfico de canalización SSH y lo bloquea.

En la mayoría de los grupos de usuarios, es posible que no permita el tráfico SSH en el centro de datos. Por lo general, SSH se usa para el acceso remoto a servidores, que no es una capacidad que desee que la mayoría de los usuarios tenga debido a que expone a los servidores del centro de datos a grandes riesgos, para acceder a servidores Linux y transferir archivos. No se puede descifrar el tráfico SSH, de modo que nadie que use SSH para acceder a los recursos del centro de datos es fiable, y aún así, se deben adjuntar todos los perfiles de amenazas a las reglas que permitan acceso a SSH para analizar en busca de malware, virus, spyware, etc.

Un ejemplo de caso de uso de SSH es el personal de TI que gestiona y realiza el mantenimiento de los servidores del centro de datos y usa SSH para el acceso remoto.



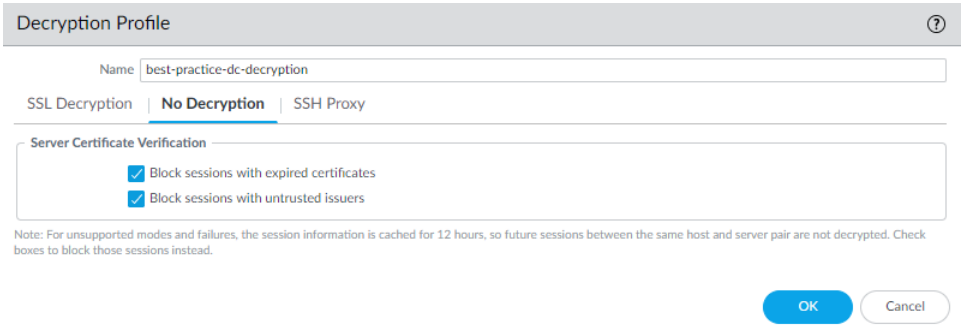
- **Comprobaciones de modo no admitidas:** el cortafuegos no puede descifrar las versiones y los cifrados de sesiones que el cortafuegos no admite, y es posible que las versiones y cifrados no admitidos sean vulnerables. Para evitar que los atacantes usen versiones y cifrados no admitidos para acceder sigilosamente a la red, bloquee las versiones y los conjuntos de cifrado de las sesiones que el cortafuegos no admite. Además, bloquear las sesiones con comprobaciones de modo no admitidas protege contra puertas traseras malintencionadas y otras amenazas que usan cifrado personalizado y no estándar para ofuscar sus actividades.
- **Comprobaciones de fallos:** si no selecciona **Block sessions if resources not available (Bloquear sesiones si los recursos no están disponibles)**, el riesgo es que la falta de recursos de procesamiento puede permitir conexiones potencialmente peligrosas. Si bloquea sesiones con recursos no

disponibles, es posible que afecte la experiencia del usuario. Implementar o no las comprobaciones de fallas depende de la posición de cumplimiento de seguridad de su empresa y de la importancia que su empresa le dé a la experiencia de usuario, en comparación con una seguridad más estricta.

STEP 6 | En el caso del tráfico que decide no descifrar, configure los ajustes de **No Decryption (Sin descifrado)** para bloquear las sesiones cifradas en los sitios con certificados vencidos o emisores que no sean de confianza.

Aplique el perfil No Decryption (Sin descifrado) únicamente al tráfico que decide no descifrar debido a la reglamentación o las reglas de cumplimiento, no al tráfico que no se puede descifrar debido a motivos técnicos, como un certificado anclado (añada ese tráfico a la lista de exclusión de descifrado SSL). Se recomienda descifrar cuanto tráfico del centro de datos sea posible.

No adjunte un perfil de configuración sin cifrado a las políticas de descifrado para el tráfico TLSv1.3 que no descifre. A diferencia de las versiones anteriores, TLSv1.3 cifra la información del certificado, por lo que el cortafuegos no tiene visibilidad de los datos del certificado y, por lo tanto, no puede bloquear sesiones con certificados caducados o emisores que no sean de confianza, por lo que el perfil no tendrá ningún efecto. (El cortafuegos puede realizar comprobaciones de certificados con TLSv1.2 y versiones anteriores, ya que esos protocolos no cifran la información del certificado y debe aplicar un perfil de configuración sin cifrado a su tráfico). Sin embargo, debe crear una política de descifrado para el tráfico TLSv1.3 que no descifre porque el cortafuegos no registra el tráfico no cifrado a no ser que una política de descifrado controle ese tráfico.



Exclusión del tráfico inadecuado del descifrado del centro de datos

Existen dos tipos de tráfico que no pueden descifrarse:

- El tráfico que anula el descifrado debido a motivos técnicos, como usar autenticación de certificado cliente, un certificado anclado o una cadena de certificados incompleta.
- Tráfico que decide no descifrar.

El cortafuegos brinda una lista predefinida de exclusión de descifrado SSL (**Device [Dispositivo] > Certificate Management [Gestión de certificados] > SSL Decryption Exclusion [Exclusión de descifrado SSL]**) para los sitios más comunes que anulan el descifrado debido a motivos técnicos. Puede eliminar sitios predefinidos de la lista haciendo clic en la casilla de verificación junto al nombre de host del sitio y haciendo clic en **Disable (Deshabilitar)**, y puede añadir sitios a la lista. Use la lista de exclusión de descifrado únicamente en los sitios que anulen el descifrado por motivos técnicos, no la use en sitios que decide no descifrar. Si el descifrado interrumpe una aplicación importante, añádala a la lista de exclusión de descifrado para crear una excepción para la dirección IP, dominio o nombre común específico en el certificado asociado a la aplicación. Es posible que algunas aplicaciones personalizadas internas se anulen si las descifra.

Si el Perfil de descifrado permite **Unsupported Modes (Modos no admitidos)** (sesiones con autenticación de cliente, versiones no compatibles o conjuntos de cifrado no compatibles), el cortafuegos añade

automáticamente servidores y aplicaciones que utilizan los modos no compatibles permitidos a su Local Decryption Exclusion (Exclusión de descifrado local) [**Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **SSL Decryption Exclusion (Exclusión de descifrado SSL)** > **Show Local Exclusion Cache (Mostrar caché de exclusión local)**]. Cuando se bloquean los modos no admitidos, aumenta la seguridad, pero también se bloquea la comunicación con aplicaciones que usan esos modos.

Si el motivo técnico para excluir un sitio del descifrado es una cadena de certificados incompleta, puede utilizar la información del log de descifrado para reparar la cadena de certificados incompleta *de modo que pueda permitir, descifrar e inspeccionar el tráfico.*

Puede decidir no descifrar el tráfico por motivos como la reglamentación o el cumplimiento legal. Por ejemplo, el Reglamento general de protección de datos (General Data Protection Regulation, GDPR) de la Unión Europea (European Union, EU) requerirá la protección sólida de los datos personales de todas las personas. El GDPR afecta a todas las empresas, incluidas las extranjeras, que recopilan o procesan los datos personales de los residentes en la UE. Las diferentes reglas de cumplimiento y normativas pueden tratar los mismos datos de manera distinta en diferentes países o regiones. Las empresas generalmente pueden descifrar información en sus centros de datos corporativos porque la empresa tiene la propiedad de la información. Lo mejor es descifrar tanto tráfico como sea posible de modo que pueda verlo y aplicar la protección de seguridad apropiada en él.

En el caso del tráfico que decide no descifrar, asegúrese de que sea tráfico que no desea descifrar y cree una exclusión basada en la política que especifique la aplicación, el grupo de usuarios, el origen y destino, la categoría de URL o el servicio para limitar cada exclusión cuanto sea posible. Cuanto más específica sea la exclusión del descifrado, mejor, de modo que no excluye de manera inadvertida más tráfico del necesario.

Creación de una estrategia de segmentación de centro de datos

Una red plana sin segmentar es difícil de defender debido a que si un atacante logra acceder a la red, el atacante podrá moverse de forma lateral y arriesgar sistemas críticos. Esto es especialmente cierto en el centro de datos, donde las empresas guardan sus activos más valiosos. Los métodos de segmentación anteriores como las VLAN no se adaptan adecuadamente, son difíciles de automatizar, y no tienen en cuenta a los usuarios, el contenido o las aplicaciones, de modo que brindan poco control o visibilidad del tráfico.

Cree una estrategia de segmentación que brinde control de acceso más detallado hacia los recursos del centro de datos, lo que le ofrece mayor visibilidad del tráfico. Cuanto más detallada es su estrategia de segmentación, más visibilidad del tráfico obtiene debido a que el tráfico debe atravesar un cortafuegos (puerta de enlace de segmentación) a medida que fluye entre los segmentos. La segmentación también facilita el cumplimiento y las auditorías debido a que puede evitar todo el acceso excepto el necesario a la información personal, lo que protege a los datos y reduce el alcance de las auditorías.

La estrategia de segmentación del centro de datos depende de la arquitectura y los objetivos comerciales, de modo que no existe una implementación estándar para todos los casos. Sin embargo, obtener información sobre las directrices comunes le permite diseñar e implementar una estrategia de segmentación para proteger su red de centro de datos.

Segmentación del centro de datos

La manera en la que segmenta el centro de datos depende de los requisitos empresariales y la arquitectura de red del centro de datos, que incluye la solución de SDN, que puede indicar el método de segmentación. Por ejemplo, las interfaces vwire controlan la conectividad del cortafuegos en un host NSX. Debido a que las interfaces vwire no enrutan ni intercambian tráfico en un host NSX, deben pertenecer a la misma zona, de modo que todos los recursos de un usuario determinado (departamento, cliente o nivel de aplicación) residan en una zona y el cortafuegos use grupos de direcciones dinámicas para segmentar el tráfico de la aplicación en esa zona. Cada usuario posee una zona diferente con sus propias interfaces vwire. En el caso de otras soluciones de SDN, es posible que diferentes instancias de cortafuegos virtuales segmenten tráfico.

Los cortafuegos Palo Alto Networks de última generación brindan herramientas flexibles para segmentar el tráfico:

- **Zonas**: el tráfico que cruza zonas atraviesa el cortafuegos para que lo inspeccione. Toda la comunicación del centro de datos permitida debe atravesar el cortafuegos y una inspección de amenazas completa (antivirus, antispyware, protección de vulnerabilidades, bloqueo de archivos, análisis de WildFire y filtrado de URL del tráfico del centro de datos que abandona la empresa y las aplicaciones alojadas por usuarios clientes). De manera predeterminada, el cortafuego bloquea todo el tráfico entre las zonas (tráfico de intrazona). Debe crear reglas específicas en la política de seguridad para permitir que el tráfico pase por las zonas, de modo que el tráfico que permite explícitamente pueda moverse de una zona a otra. La manera en la que use las zonas para segmentar el centro de datos depende de los activos que debe separar de otros activos. Por ejemplo, una arquitectura común incluye zonas diferentes para los servidores de desarrollo y los servidores de producción. Puede usar zonas para segmentar servidores que alojan información extremadamente confidencial como información de la tarjeta de pago (Payment Card Information, PCI) o información personal identificatoria (Personally Identifiable Information, PII) para segmentar diferentes departamentos internos de la empresa como el de marketing, ingeniería y recursos humanos, y para segmentar los recursos del cliente y las aplicaciones que aloja el cliente.

Considere usar perfiles de protección de zonas para proteger las zonas de inundaciones, actividades de reconocimiento (análisis de puertos y limpieza de host), ataques basados en paquetes de capa 3 y basados en paquetes de protocolo no IP (capa 2).

- **Grupos de direcciones dinámicas**: con este fin, los grupos de direcciones dinámicas son listas de direcciones IP que el cortafuegos importa y usa en la política de seguridad para definir los grupos de servidores de manera dinámica, en lugar de hacerlo de manera estática. Añadir y eliminar direcciones IP de un grupo de direcciones dinámicas actualiza la política de seguridad automáticamente, sin necesidad de una confirmación en el cortafuegos. Dentro de una zona, el uso de grupos de direcciones dinámicas en las reglas de permiso de la política de seguridad permite la interacción entre servidores de aplicaciones y servicios especificados. Por ejemplo, en NSX, use grupos de direcciones dinámicas para segmentar los niveles de servidor en un nivel de aplicación.
- **User-ID**: permite que User-ID cree reglas de aplicaciones permitidas basadas en los grupos de usuario para segmentar usuarios de aplicaciones y grupos de servidores.

Cuando diseñe el plan de segmentación del centro de datos, tenga en cuenta las siguientes directrices generales:

- La evaluación del centro de datos, de modo que pueda segmentarlo en etapas y proteger los activos más valiosos y confidenciales primero.
- Use una solución de SDN (como NSX, ACI, OpenStack) en el centro de datos para brindar una infraestructura escalable, ágil y virtualizada. Las SDN son la mejor manera de centralizar la gestión de la red del centro de datos, maximizar el uso de los recursos de procesamiento, escalar y automatizar la red, y controlar y proteger el tráfico en una red virtualizada. A pesar de que puede crear una arquitectura sin SDN que imite, en esencia, a una arquitectura con SDN, es difícil y requiere tiempo, es propenso a errores que pueden causar una caída del servicio y no se recomienda. Las soluciones de SDN maximizan el uso de los recursos de procesamiento subyacentes del centro de datos sin sacrificar la seguridad.
- Use cortafuegos físicos de última generación para segmentar y proteger los servidores heredados no virtualizados, y usar los cortafuegos serie VM para segmentar y proteger la red virtual del centro de datos.
- Agrupe activos que funcionen de manera similar y requieran el mismo nivel de seguridad en el mismo segmento del centro de datos. Por ejemplo, ubique a los servidores que se conectan a internet en el mismo segmento.

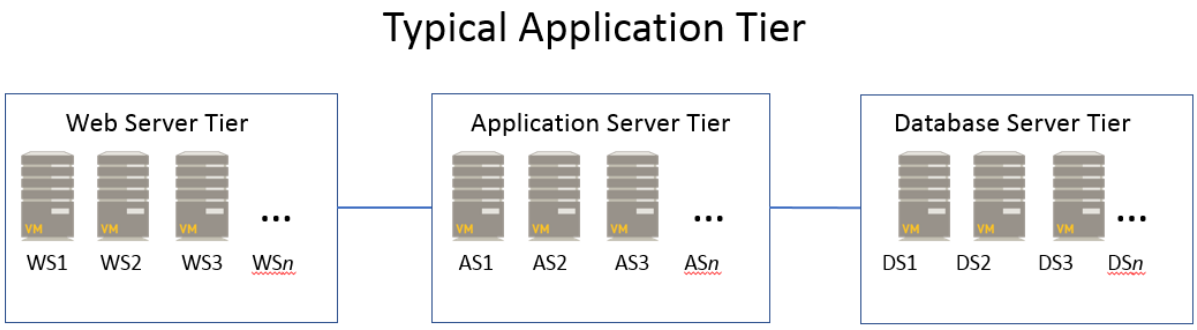
Base su plan de segmentación en varios criterios para desarrollar el plan adecuado y proteger su negocio.

Segmentación de las aplicaciones del centro de datos

Segmente aplicaciones del centro de datos para evitar que el malware se mueva entre aplicaciones y para permitir de manera segura esas aplicaciones para los usuarios. Los *niveles de aplicaciones* brindan los recursos y las funciones necesarias para las aplicaciones en el centro de datos. Un nivel de aplicación incluye varios *niveles de servidor* que funcionan en conjunto para realizar solicitudes y comandos relacionados con una aplicación determinada. Por lo general, un nivel de aplicación consta de tres niveles de servidor:

- *Nivel de servidor web*: interfaz de la aplicación para los usuarios.
- *Nivel de servidor de la aplicación*: recibe solicitudes del nivel de servidor web para procesar y generar funcionalidades de la aplicación.
- *Nivel de servidor de la base de datos*: contiene datos que la aplicación requiere para funcionar.

Cada nivel de servidor contiene servidores que funcionan de manera similar y trabajan en conjunto, de modo que un nivel de aplicación puede brindarle una aplicación a un usuario.



Los niveles de servidor en cada nivel de aplicación crean una *cadena de servicio* de VM. Las cadenas de servicio dirigen al tráfico a través de los dispositivos virtuales del centro de datos para brindar servicios de aplicaciones. En un nivel de aplicación, es posible que un servidor web se comunique con un servidor de aplicación que aloja el código de aplicación y es posible que el servidor de la aplicación se comunique con un servidor en la base de datos que aloja contenido. La comunicación entre los tres servidores, que se encuentran en diferentes niveles de servidor dentro de un nivel de aplicación, se denomina cadena de servicio.

Los centros de datos contienen varios niveles de aplicación, que pueden ser exclusivos de determinados departamentos, clientes, contratistas u otros grupos. Segmente la infraestructura de la aplicación en el centro de datos para evitar comunicaciones no autorizadas e innecesarias entre los recursos de la aplicación e inspeccionar el tráfico de la aplicación.

Segmentación de aplicaciones	Cómo segmentar aplicaciones
Nivel de aplicación	Segmente los niveles de servidor en cada nivel de aplicación configurando una zona diferente de cortafuegos para cada nivel de servidor, de modo que pueda controlar el acceso a cada conjunto de servidores y examinar el tráfico que fluye entre cada nivel de servidor a medida que atraviesa el cortafuegos. Por ejemplo, ubique los servidores web, los servidores de la aplicación y los servidores de la base de datos en zonas diferentes, de modo que el tráfico entre los niveles de servidor siempre pase por un cortafuegos de última generación y se inspeccione completamente. Según los requisitos empresariales, es posible que deba crear más de una zona por nivel de aplicación para separar a los usuarios, equilibrar la carga, usar niveles de aplicación con diferentes fines, brindar diferentes niveles de seguridad o conectarse a diferentes conjuntos de servidores. Segmente el centro de datos para reducir la superficie de ataque de cada nivel de aplicación agrupando en la misma zona únicamente los servidores que requieren niveles similares de confianza y que deben comunicarse con niveles de aplicación similares.
Nivel de servidor web	Por lo general, el tráfico accede al centro de datos a través de los servidores web, pero existen casos especiales, como cuando el departamento de TI configura un acceso directo seguro a los servidores del centro de datos por motivos de gestión. Como en el resto de los niveles de servidor, cree una zona separada para el nivel de servidor web, de modo que pueda aplicarle una política de seguridad detallada. Debido a que el nivel de servidor web se comunica con los dispositivos que residen fuera del centro de datos, es un objetivo atractivo para los atacantes. Ubique el nivel de servidor web en una red diferente, por ejemplo, usando una VLAN. Todo el tráfico de entrada o salida de la VLAN (todo el tráfico que acceda o salga del centro de datos) debe atravesar un cortafuegos de última generación. Puede

Segmentación de aplicaciones	Cómo segmentar aplicaciones
	hacerlo configurando el cortafuegos de última generación como la puerta de enlace predeterminada o usando una solución de SDN como NSX para dirigir el tráfico. Segmente los servidores en el nivel de servidor web para evitar que se comuniquen entre sí, por ejemplo, usando una regla tradicional como el *cortafuegos distribuido (Distributed Firewall, DFW) de NSX* para abrir un puerto o bloquear el tráfico en el nivel.
Servidores de aplicación del servicio de infraestructura	Segmente los servidores que brindan servicios de infraestructura críticos como DNS, DHCP y NTP, y permita el acceso únicamente a sus direcciones IP específicas, usando únicamente las aplicaciones adecuadas.
applications	Use App-ID para crear reglas de permiso basadas en aplicaciones para la política de seguridad que segmenten las aplicaciones controlando quién puede acceder a cada aplicación y en qué conjuntos de servidores (usando grupos de direcciones dinámicas). App-ID le permite aplicar reglas detalladas de la política de seguridad a aplicaciones que pueden residir en el mismo recurso de procesamiento, pero requieren diferentes niveles de seguridad y control de acceso. Cree aplicaciones personalizadas para identificar las aplicaciones exclusivas y segmentar el acceso. Si posee políticas existentes de cancelación de aplicaciones que creó únicamente para definir los tiempos de espera personalizados de una sesión en un conjunto de puertos, convierta las políticas existentes de cancelación de aplicaciones en políticas basadas en la aplicación configurando los tiempos de espera de una sesión basados en el servicio para conservar el tiempo de espera personalizado de cada aplicación y migrar la regla a una regla basada en la aplicación. Las políticas de cancelación de aplicaciones se basan en los puertos. Cuando usa políticas de cancelación de aplicaciones para conservar los tiempos de espera personalizados de una sesión en un conjunto de puertos, pierde visibilidad de la aplicación respecto a esos flujos, de modo que no sabe ni controla las aplicaciones que usan los puertos. Los tiempos de espera de una sesión basados en el servicio logran tiempos de espera personalizados y conservan la visibilidad de la aplicación. Para migrar de una política de seguridad basada en el puerto con valores de tiempo de espera de la aplicación personalizados a una política basada en la aplicación, no use reglas de cancelación de aplicación para conservar los valores de tiempo de espera personalizados debido a que perderá la visibilidad de las aplicaciones. En cambio, defina un tiempo de espera para la sesión basado en el servicio a fin de conservar el tiempo de espera personalizado para cada aplicación y migre la regla a una regla basada en la aplicación.

No use cortafuegos de última generación para segmentar servidores en un nivel de servidor específico. Cuando desee evitar la intercomunicación de los servidores en un nivel de servidor, use una regla tradicional como el DFW de NSX para abrir un puerto o bloquear el tráfico en el nivel. Sin embargo, los servidores en un nivel de servidor, generalmente, necesitan comunicarse entre sí. Por ejemplo, es posible que un nivel de servidor de la base de datos sea un clúster que requiere intercomunicación libre.

Creación de perfiles de seguridad recomendados para el centros de datos

Los perfiles de seguridad brindan protección fundamental mediante la detección de amenazas en el tráfico que permite en la red. Los perfiles de seguridad ofrecen un conjunto completo de herramientas de prevención de amenazas coordinadas que bloquea el tráfico de aplicaciones de mando y control (command and control, C2) entre peers, tipos de archivos peligrosos, intentos de aprovechar las vulnerabilidades y firmas de antivirus, además de identificar malware nuevo y desconocido.

Requiere un esfuerzo relativamente bajo aplicar los perfiles de seguridad debido a que Palo Alto Networks brinda perfiles predefinidos que puede añadir a las reglas de permiso de la política de seguridad. Personalizar perfiles de seguridad es sencillo debido a que puede clonar un perfil predefinido y editarlo. Por supuesto, puede crear un perfil de seguridad completamente en el cortafuegos o en Panorama.

Para detectar amenazas conocidas y desconocidas en el tráfico de tu red, adjunte perfiles de seguridad a todas las reglas en la política de seguridad que permiten el tráfico hacia la red, de modo que el cortafuegos inspeccione todo el tráfico permitido. El cortafuegos aplica perfiles de seguridad al tráfico que coincide con la regla de permiso de la política de seguridad, analiza el tráfico según los ajustes del perfil de seguridad y toma las medidas adecuadas para proteger la red. Los perfiles de seguridad recomendados se aplican en los cuatro flujos de tráfico en el centro de datos, a excepción de lo que se indique.

Descargue las actualizaciones de contenido automáticamente e instálelas lo antes posible, de modo que cuente con el contenido y las firmas de prevención de amenazas más recientes (antivirus, antispyware, vulnerabilidades, malware, etc.) en el cortafuegos y pueda bloquear las amenazas más recientes.

- Creación de perfiles de antivirus recomendados para el centro de datos
- Creación de perfiles antispyware recomendados para el centro de datos
- Creación de perfiles de protección contra vulnerabilidades recomendados para el centro de datos
- Creación de perfiles de bloqueo de archivos recomendados para el centro de datos
- Creación de perfiles de análisis de WildFire recomendados para el centro de datos

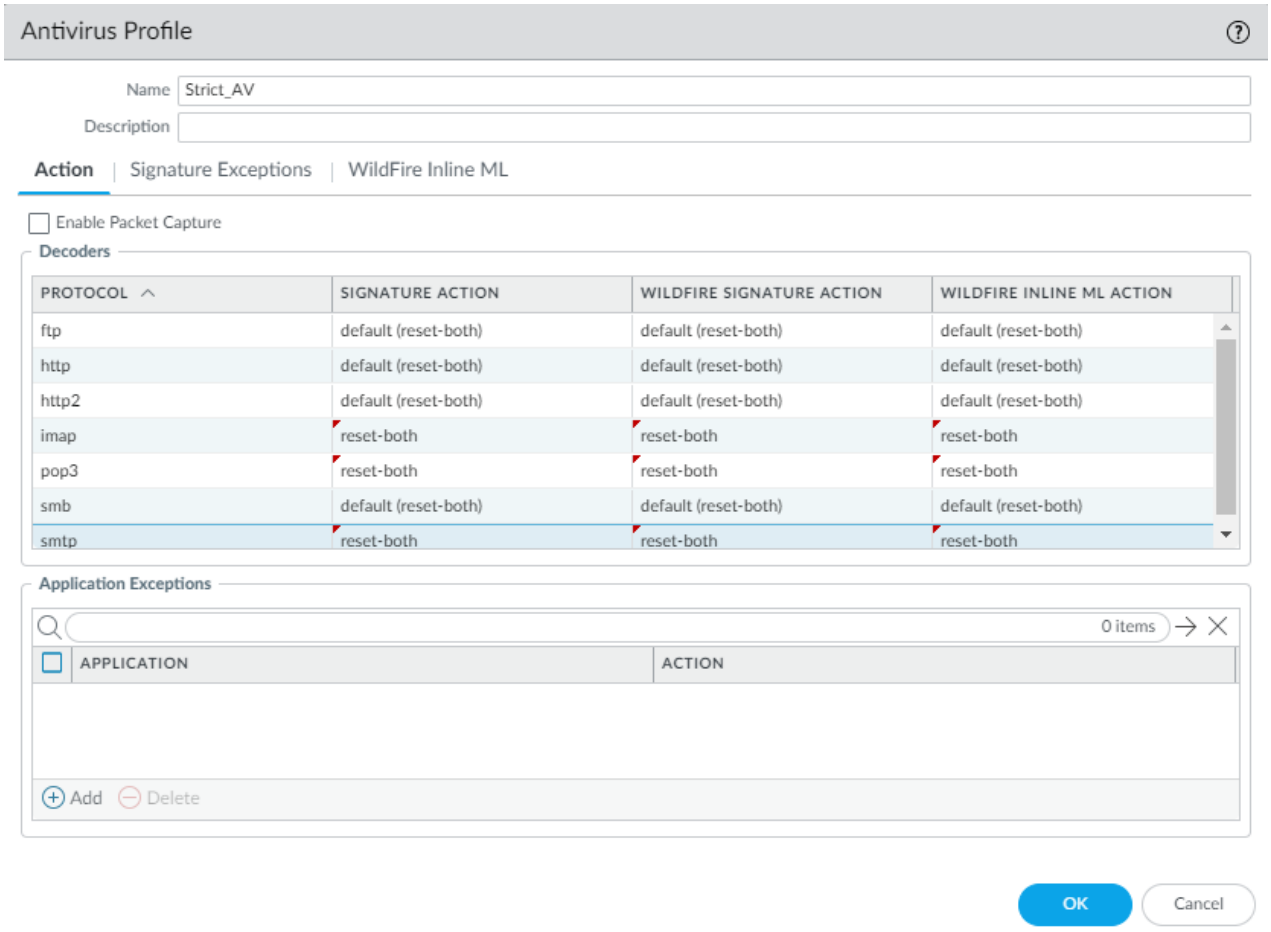
Cree uno o más Grupos de perfiles de seguridad para que pueda aplicar todos los perfiles a una regla de política de seguridad a la vez en lugar de hacerlo individualmente.

No necesita una suscripción de filtrado de URL para los cortafuegos del centro de datos si no existe una conexión de salida directa a internet. Los cortafuegos que no se conectan directamente a internet no requieren la solución de filtrado de URL PAN-DB debido a que identifica URL de internet, no URL privadas del centro de datos, de modo que importar la base de datos de PAN-DB y comprobar las URL con ella no se aplica al tráfico del centro de datos. Si no está seguro de si el cortafuegos tiene tráfico de URL, obtenga una suscripción de prueba de filtrado de URL y configure el perfil para alertar sobre todas las categorías de URL a fin de identificar el tráfico de URL. De lo contrario, el filtrado de URL debe realizarse en el cortafuegos en el perímetro de la red donde el tráfico de usuario entra y sale de la red, no en el perímetro del centro de datos. Considere crear categorías personalizadas de URL (**Objects [Objetos]** > **Custom Objects [Objetos personalizados]** > **URL Category [Categoría de URL]**) para identificar y controlar el acceso a los servicios de los servidores web del centro de datos.

Creación de perfiles de antivirus recomendados para el centro de datos

Duplique el perfil de antivirus predeterminado y edítelo. Para garantizar la disponibilidad para aplicaciones críticas para el negocio, siga los pasos para una transición segura a medida que pasa de su estado actual al perfil de prácticas recomendadas. Para conseguir el mejor perfil de prácticas recomendadas, modifique el perfil de antivirus predeterminado como se muestra aquí y adjúntelo a todas las reglas de la política de seguridad que permiten el tráfico. El perfil de antivirus posee decodificadores de protocolos que detectan y evitar que los virus y malware se transfieran a través de siete protocolos: FTP, HTTP, HTTP2, IMAP, POP3, SMB y SMTP. Puede establecer acciones de WildFire para los seis protocolos debido a que el perfil de antivirus también aplica acciones basadas en las firmas de WildFire y el aprendizaje automático en línea.

Configure el perfil de antivirus recomendado clonado para restablecer el cliente y el servidor para los siete decodificadores de protocolo y las acciones de WildFire, y adjunte el perfil a las reglas de permitidos para los cuatro flujos de tráfico en el centro de datos.



Los triángulos rojos en la esquina superior izquierda de una celda indican que la acción se modificó (se cambió el valor predeterminado) y el nombre del perfil modificado es **Strict_AV**.

Adjunte el perfil de antivirus recomendado a todas las reglas en la política de seguridad que permiten que el tráfico bloquee archivos malintencionados conocidos (malware, bots de ransomware y virus) cuando intenten ingresar a la red. Por ejemplo:

- Tráfico dentro del centro de datos: el perfil de antivirus, junto con el perfil de protección de vulnerabilidades, ayuda a evitar que los atacantes usen vulnerabilidades de seguridad para aprovechar las

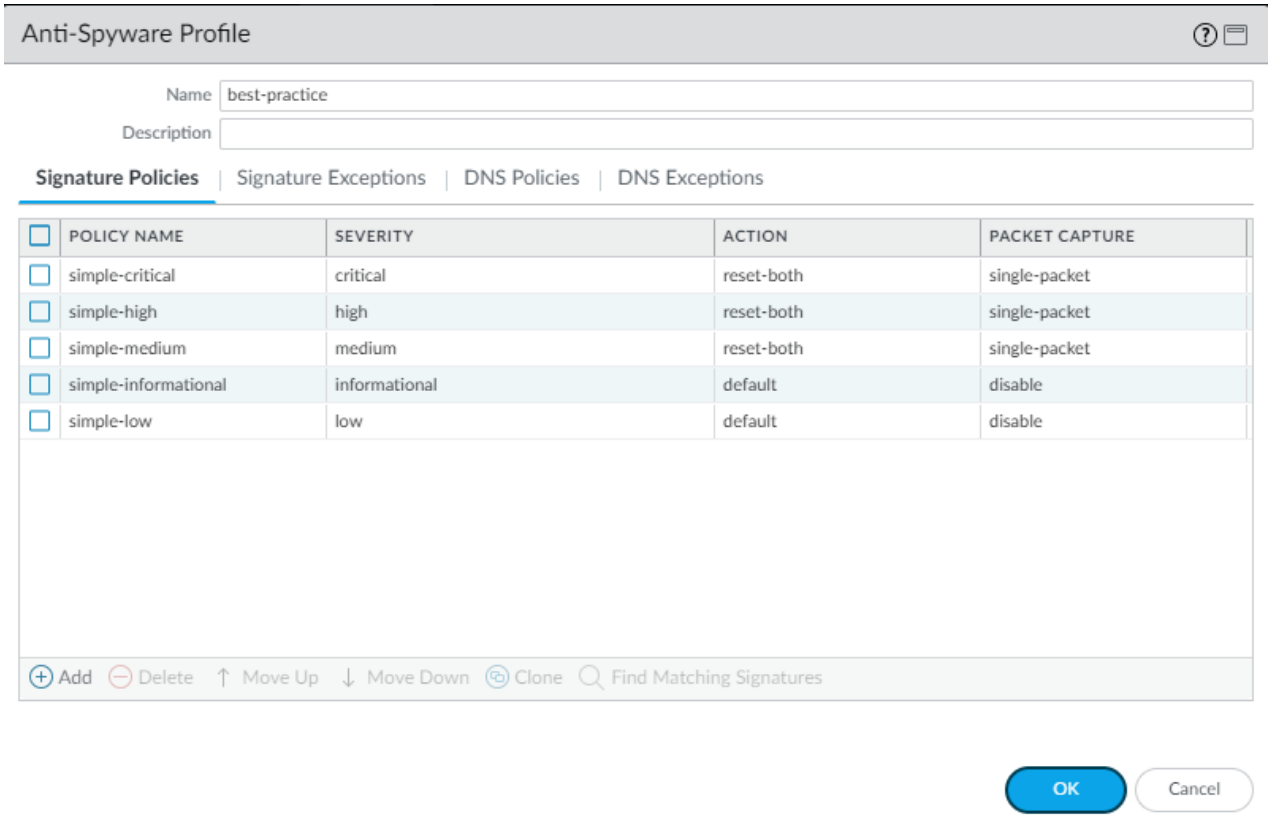
vulnerabilidades, y propagar malware y herramientas de hacking lateralmente entre los servidores dentro de la red del centro de datos.

- Tráfico desde el centro de datos hacia internet: el perfil de antivirus, junto con el perfil antispyware, ayuda a identificar y bloquear tráfico de mando y control y descargas iniciales de malware o herramientas de hacking.

Creación de perfiles antispyware recomendados para el centro de datos

Adjunte un perfil de antispyware a todas las reglas de la política de seguridad que permiten tráfico en el centro de datos. El perfil antispyware detecta tráfico de mando y control (C2) que inicia a partir de spyware instalado en un servidor o endpoint, que incluye categorías como adware, puertas traseras, secuestro de navegador, robo de datos y captura de pulsaciones, y evita que los sistemas en riesgo establezcan una conexión de salida desde su red.

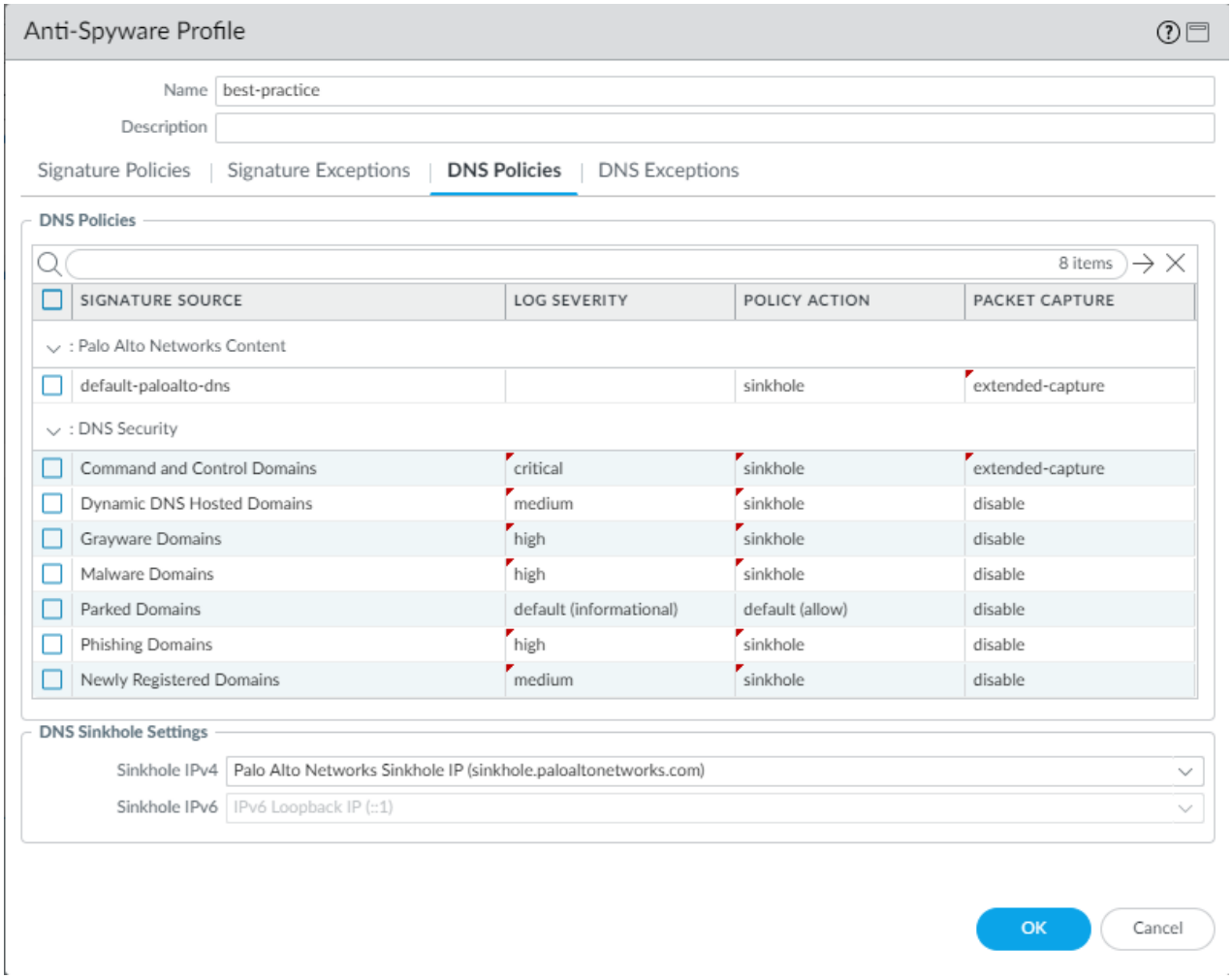
Duplique el perfil antispyware estricto predefinido y edítelo. Para garantizar la disponibilidad para aplicaciones críticas para el negocio, siga los pasos para una transición segura a medida que pasa de su estado actual al perfil de prácticas recomendadas. Si configuró un sinkhole al que puede enviar tráfico para analizarlo, habilite el sinkhole DNS con captura de paquetes para ayudar a realizar un seguimiento del endpoint que intentó determinar el dominio malintencionado. El perfil antispyware recomendado conserva la **Action (Acción)** predeterminada para restablecer la conexión cuando el cortafuegos detecta una amenaza de seguridad de gravedad intermedia, alta o crítica, y habilita la captura de un solo paquete (packet capture, PCAP) para esas amenazas.



No habilite la PCAP para la actividad informativa debido a que genera un volumen relativamente elevado de tráfico y no es útil en comparación con las posibles amenazas. Aplique PCAP amplia (opuesta a la PCAP única) al tráfico de valor elevado al que aplica la Action (Acción) **alert (alertar)**. Aplique la PCAP usando la misma lógica que usa para decidir qué trafico registrar; tome PCAP del tráfico que registra. Aplique PCAP

única al tráfico que bloquea. El número predeterminado de paquetes que registra y envía un PCAP amplio al plano de gestión es de cinco paquetes, que es el valor recomendado. En la mayoría de los casos, capturar cinco paquetes brinda suficiente información para analizar la amenaza. Si se envía demasiado tráfico de PCAP al plano de gestión, capturar más de cinco paquetes puede provocar el descarte de PCAP.

La **Action on DNS Queries (Acción en caso de una solicitud DNS)** recomendada es bloquear o sinkhole solicitudes DNS de dominios malintencionados conocidos y cuando no cuenta con visibilidad de las solicitudes DNS, y habilitar las PCAP.



Habilitar el sinkhole DNS permite identificar los hosts potencialmente en riesgo que intentan acceder a dominios sospechosos realizando el seguimiento de los hosts y evitando que accedan a esos dominios. Habilite el sinkhole DNS cuando el cortafuegos no vea al creador de la solicitud DNS (por lo general, cuando el cortafuegos se encuentra antes del servidor DNS local), de modo que pueda identificar los hosts infectados. No habilite el sinkhole DNS cuando el cortafuegos pueda ver al creador de la solicitud DNS (por lo general, cuando el cortafuegos se encuentra después del servidor DNS local; en este caso, las reglas de bloqueo y los logs del cortafuegos brindan visibilidad del tráfico) o el tráfico que bloquea.

Además de proteger los hosts con sinkhole DNS, adjunte el perfil antispyware recomendado a todas las reglas de la política de seguridad que permiten el tráfico para identificar a los hosts infectados cuando el tráfico abandona la red y detener a los atacantes evitando que los sistemas en riesgo se comuniquen con la red de C2 malintencionada. Si un sistema no se puede comunicar con la red de C2, la red de C2 no puede controlar el sistema. Por ejemplo:

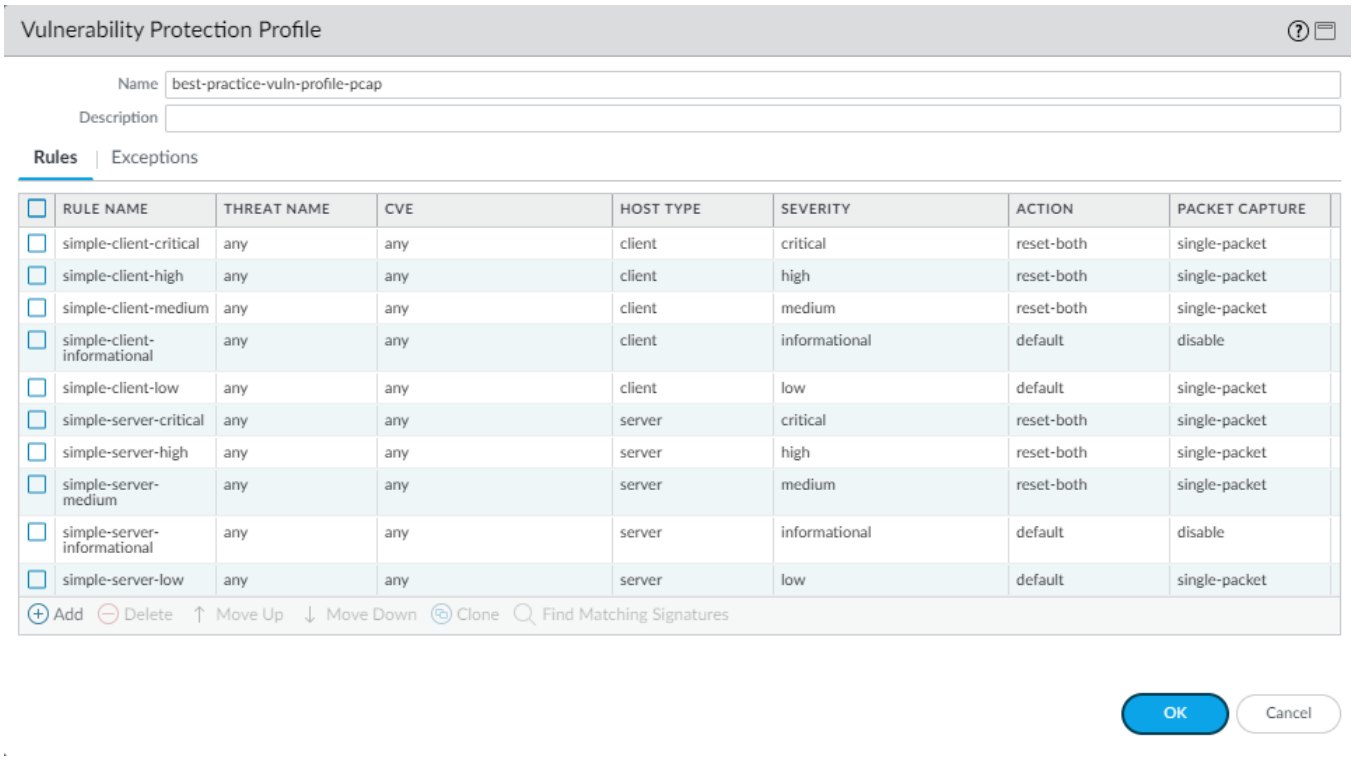
- Tráfico desde los usuarios hacia el centro de datos, tráfico en el centro de datos y tráfico desde internet hacia el centro de datos: el perfil antispyware bloquea el tráfico de C2 entre peers.

- Tráfico desde el centro de datos hacia internet: el perfil antispyware, junto con el perfil de antivirus, ayuda a identificar y bloquear tráfico de C2 y descargas iniciales de malware o herramientas de hacking.

Creación de perfiles de protección contra vulnerabilidades recomendados para el centro de datos

Adjunte un perfil de protección de vulnerabilidades a todas las reglas de la política de seguridad que permiten tráfico. El perfil de protección de vulnerabilidades protege de desbordamientos de búfer, ejecución ilegal de códigos y otros intentos de aprovechar las vulnerabilidades en el lado del cliente y del servidor para filtrarse y moverse lateralmente en la red del centro de datos.

Clone el perfil de protección de vulnerabilidades estricto predefinido. Para garantizar la disponibilidad para aplicaciones críticas para el negocio, siga los pasos para una transición segura a medida que pasa de su estado actual al perfil de prácticas recomendadas. Para el mejor perfil de prácticas recomendadas, para cada regla a excepción de **simple-client-informational** y **simple-server-informational**, haga doble clic en **Rule Name (Nombre de la regla)** y modifique **Packet Capture (Captura de paquetes)** de **disable (deshabilitar)** a **single-packet (paquete único)** para habilitar la captura de paquetes (PCAP) en cada regla, de forma que pueda controlar el origen de posibles ataques. No modifique el resto de los ajustes. Descargue actualizaciones de contenido automáticamente e instálelas cuanto antes, de modo que la firma siempre permanezca actualizada.



No habilite la PCAP para la actividad informativa debido a que genera un volumen relativamente elevado de tráfico y no es útil en comparación con las posibles amenazas. Aplique PCAP amplia (opuesta a la PCAP única) al tráfico de valor elevado al que aplica la Action (Acción) **alert (alertar)**. Aplique la PCAP usando la misma lógica que usa para decidir qué trafico registrar; tome PCAP del tráfico que registra. Aplique PCAP única al tráfico que bloquea. El número predeterminado de paquetes que registra y envía un PCAP amplio al plano de gestión es de cinco paquetes, que es el valor recomendado. En la mayoría de los casos, capturar cinco paquetes brinda suficiente información para analizar la amenaza. Si se envía demasiado tráfico de PCAP al plano de gestión, capturar más de cinco paquetes puede provocar el descarte de PCAP.

El motivo de adjuntar el perfil recomendado de protección de vulnerabilidades a todas las reglas de la política de seguridad que permiten tráfico es que si no cuenta con una protección de vulnerabilidades estricta, los atacantes pueden aprovechar las vulnerabilidades del lado del cliente y del servidor para poner el centro de datos en riesgo. Por ejemplo:

- Tráfico dentro del centro de datos: el perfil de protección de vulnerabilidades estricto, junto con el perfil de antivirus, ayuda a evitar que los atacantes usen vulnerabilidades de seguridad para aprovechar las vulnerabilidades, y propagar malware y herramientas de hacking lateralmente entre los servidores dentro de la red del centro de datos.
- Tráfico desde el centro de datos hacia internet: la protección de vulnerabilidades permite evitar que los servidores infectados del centro de datos pongan a los servidores de internet en riesgo.
- Tráfico desde internet hacia el centro de datos: un perfil de protección de vulnerabilidades estricto bloquea los intentos de poner a los servidores del centro de datos en riesgo con vulnerabilidades en el lado del servidor. Si un servidor se encuentra en riesgo, la protección de vulnerabilidades permite evitar que el servidor infectado envíe vulnerabilidades de seguridad a los clientes, aísla la infección y protege a sus socios y clientes contra los ataques de abrevadero. La protección de vulnerabilidades también detiene ataques de fuerza bruta usando la acción Block IP (Bloquear IP). Cuando las firmas de ataque de fuerza bruta activan la acción, el cortafuegos bloquea la dirección IP del atacantes por un período de tiempo configurado. Si el ataque de fuerza bruta continúa tras este período de tiempo, las firmas vuelven a activar la acción de bloqueo. Es posible que el ataque de fuerza bruta continúe, pero nunca será exitoso.

Creación de perfiles de bloqueo de archivos recomendados para el centro de datos

Use el perfil de bloqueo de archivos estricto predefinido para bloquear los archivos que se incluyen comúnmente en las campañas de ataque de malware o que no tienen un caso de uso real para la carga/descarga. Bloquear estos archivo reduce la superficie de ataque. El perfil predefinido estricto bloquea los archivos por lotes, DLL, archivos de clase Java, archivos de ayuda, accesos directos de Windows (.lnk), archivos .rar, archivos .tar, archivos cifrados rar y zip, archivos codificados de varios niveles (archivos codificados o comprimidos hasta cuatro veces), archivos .hta, y archivos portable ejecutable (Portable Executable, PE) de Windows, que incluyen archivos .exe, .cpl, .dll, .ocx, .sys, .scr, .drv, .efi, .fon y .pif. El perfil predefinido alerta sobre todos los demás tipos de archivos para brindar visibilidad de otras transferencias de archivo que puede determinar si desea introducir cambios en la política.

En algunos casos, es posible que la necesidad de admitir aplicaciones críticas evite que bloquee todos los tipos de archivos del perfil estricto. Siga el consejo para la transición segura para ayudar a determinar si necesita hacer excepciones en diferentes áreas de la red. Revise los logs de filtrado de datos [Monitor (Supervisar) > Logs > Data Filtering (Filtrado de datos)] para identificar los tipos de archivos que se usan en el centro de datos y comunicarse con las partes interesadas en el negocio para hablar sobre los tipos de archivos que requieren sus aplicaciones. En función de esta información, de ser necesario, clone el perfil estricto y modifíquelo según sea necesario para permitir solo el otro tipo de archivos que deben admitir las aplicaciones críticas. Puede usar el ajuste de dirección para evitar que determinados tipos de archivos fluyan en ambas direcciones o para bloquear a los archivos en una dirección, pero no en otra.

NAME	LOCATION	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
basic file blocking	Predefined	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf	both	block
		Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	continue
		Log all other file types	any	any	both	alert
strict file blocking	Predefined	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
		Block encrypted files	any	encrypted-rar, encrypted-zip	both	block
		Log all other file types	any	any	both	alert

El motivo de adjuntar el perfil recomendado de bloqueo de archivos a todas las reglas de la política de seguridad que permiten tráfico es evitar que los atacantes envíen archivos malintencionados al centro de datos a través de aplicaciones de uso compartido de datos o paquetes de vulnerabilidades de seguridad, o infectando a usuarios que acceden al centro de datos, o con unidades USB.

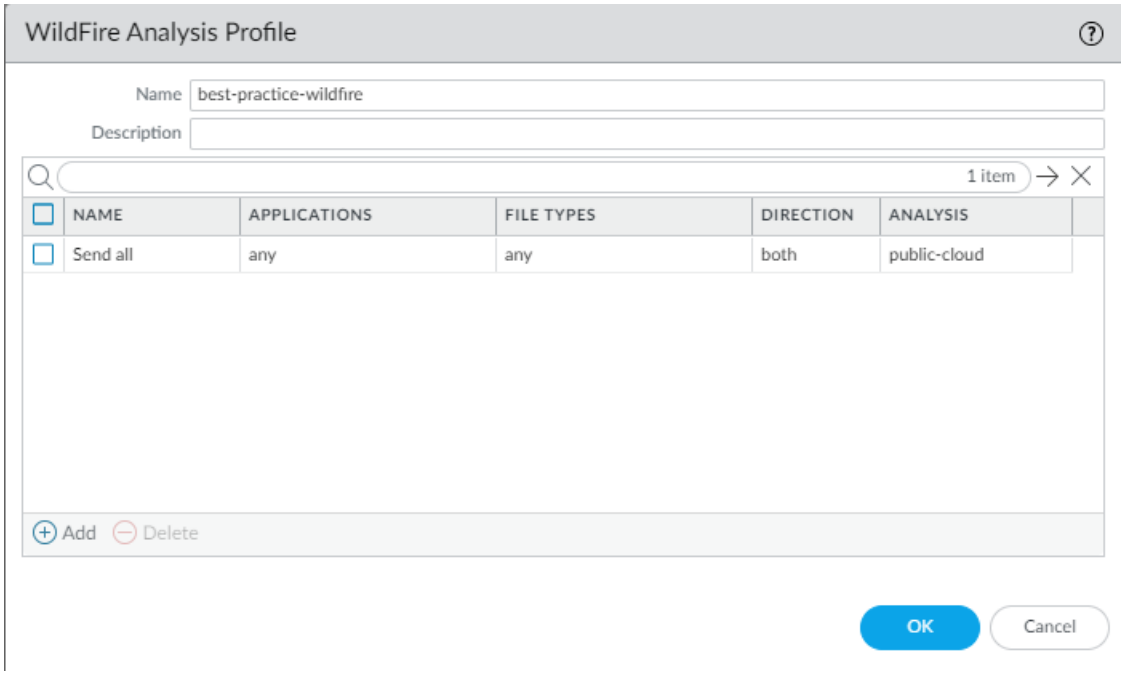
- Tráfico desde los usuarios hacia el centro de datos: adjunte el perfil de bloqueo de archivos estricto a las reglas de la política de seguridad para las aplicaciones que no incluyan uso compartido de datos o colaboración a fin de bloquear los tipos de archivos peligrosos que pueden enviar vulnerabilidades de seguridad y malware.
- Tráfico en el centro de datos: adjunte un perfil de bloqueo de archivos estricto a las reglas de la política de seguridad para evitar que un servidor en riesgo comparta un archivo malintencionado con otros servidores en el centro de datos. Esto aísla la infección y evita que el malware se propague en el centro de datos.
- Tráfico desde el centro de datos hacia internet: limite las transferencias de archivos a los tipos de archivos necesarios para la aplicación en uso.

Si no bloquea todos los archivos de Windows PE, envíe todos los archivos desconocidos a WildFire para analizarlos. Para las cuentas de usuario, establezca la **Action (acción)** en **continue (continuar)** para ayudar a evitar descargas ocultas en las que sitios web, correos electrónicos o ventanas emergentes malintencionadas provoquen que los usuarios descarguen archivos malintencionados accidentalmente. Informe a sus usuarios que si les aparece un mensaje que les indica continuar con la transferencia de un archivo que no iniciaron intencionadamente, pueden quedar sujetos a una descarga malintencionada.

Creación de perfiles de análisis de WildFire recomendados para el centro de datos

Los otros perfiles de seguridad detectan y bloquean las amenazas conocidas. WildFire protege el centro de datos contra amenazas *desconocidas*. Configure el cortafuegos para que reenvíe todos los archivos desconocidos a WildFire para su análisis usando el perfil predeterminado predefinido. Las amenazas desconocidas pueden ocultarse en diferentes tipos de archivos y es posible que los ataques exitosos no se detecten hasta que ya hayan hecho daño. Por ejemplo, WildFire puede identificar malware que se carga en un servidor escalonado antes de que el atacante pueda dañarlo, y buscar detectores de vulnerabilidad y herramientas de asistencia de movimiento lateral antes de que los atacantes logren sus objetivos. Es posible que WildFire haya evitado una cantidad de filtraciones empresariales a gran escala en los últimos años. Todas las reglas de la política de seguridad que controlen el tráfico que implicó, implicará o podría implicar actividad de transferencia de archivos debe incluir un perfil de análisis de WildFire habilitado.

Configure las actualizaciones de contenido en el dispositivo WildFire *para que se descarguen e instalen automáticamente, de modo que siempre tenga el soporte más reciente. Por ejemplo, el soporte para los archivos de Linux y SMB se entregó en las actualizaciones de contenido del dispositivo WildFire.*



El motivo para adjuntar el perfil de análisis de WildFire predeterminado a todas las reglas en la política de seguridad para permitir el tráfico es debido a que WildFire brinda la mejor defensa contra amenazas desconocidas y amenazas avanzadas persistentes (advanced persistent threats, ATP). Por ejemplo:

- El tráfico desde los usuarios hacia el centro de datos: WildFire identifica el malware desconocido alojado en el centro de datos como Confluence o SharePoint.
- Tráfico en el interior del centro de datos: WildFire identifica malware desconocido que se propaga en los servidores del centro de datos, lo que permite evitar la filtración de datos ya que el malware se descubre antes de que pueda hacer daño.
- Tráfico desde el centro de datos hacia internet: debido a que este tráfico descarga ejecutables para actualizaciones de software y sistemas operativos, es fundamental que ejecute WildFire en todas las aplicaciones para identificar comportamientos malintencionados.

Establezca alertas de malware a través de correos electrónicos, SNMP o un servidor syslog, de modo que el cortafuegos notifique automáticamente cuando encuentre un posible problema. Cuanto antes aísle un host en riesgo, menor será la probabilidad de que el malware antes desconocido se propague a otros dispositivos en el centro de datos y será más fácil solucionar el problema.

De ser necesario, puede limitar las aplicaciones y los tipos de archivos que se envían para analizar según la dirección del tráfico.

La configuración de una acción de WildFire en el perfil de antivirus puede influir en el tráfico si este genera una firma de WildFire que tenga como resultado una acción de restablecimiento o borrado. Puede excluir el tráfico interno, como aquellas aplicaciones de distribución de software a través de las cuales implementa programas de creación personalizada para realizar una transición segura a una práctica recomendada, ya que WildFire puede identificar programas de creación personalizada como maliciosos y generar una firma para ellos. Compruebe Monitor (Supervisar) > Logs (Logs) > WildFire Submissions (Envíos de Wildfire) para ver si algún programa de creación personalizada activa las firmas de WildFire.

Utilice Cortex XDR Agent para proteger los endpoints del centro de datos

Cortex XDR Agent protege a los endpoints en el centro de datos como servidores y VM contra malware y explotaciones en el endpoint, mientras que el cortafuegos de última generación protege contra las amenazas que cruzan la red (y deben atravesar el cortafuegos) para llegar al endpoint. Cuando el malware o las vulnerabilidades de seguridad ya se encuentran en el endpoint o llegan a un endpoint, si este ejecuta la amenaza (por ejemplo, con un archivo .exe o .dll), el cortafuegos no ve la amenaza porque la acción se encuentra en el endpoint y el tráfico no cruza el cortafuegos, de modo que no hay movimientos que vea el cortafuegos. Sin embargo, en cada endpoint, Cortex XDR Agent observa las amenazas en archivos ejecutables, en macros de documentos, archivos de bibliotecas de enlaces dinámicos, etc. Cuando las amenazas intentan ejecutarse, las capturas se inician en el endpoint y lo protegen.

Cortex XDR Agent y el cortafuegos de última generación brindan una protección doble a los endpoints del centro de datos; el cortafuegos protege a los endpoints de las amenazas en la red y Cortex XDR Agent supervisa y protege a los endpoints de las amenazas que residen en el endpoint. La política de seguridad que configure para los endpoints en un gestor de seguridad para endpoints (Endpoint Security Manager, ESM) y la política de seguridad que configure en Panorama o en los cortafuegos no entran en conflicto dado que rigen diferentes eventos en diferentes ubicaciones. Cortex XDR Agent controla la seguridad en cada endpoint individual. El cortafuegos controla la seguridad del tráfico que atraviesa el cortafuegos.

Instale Cortex XDR Agent en todos los endpoints del centro de datos. Las prácticas recomendadas para Cortex XDR Agent en el centro de datos son las mismas que para Cortex XDR Agent en cualquier endpoint debido a que el contexto siempre es el endpoint, de modo que el contexto "en el centro de datos" o "en el grupo de usuarios" no importa. Cortex XDR Agent protege a todos los endpoints de igual modo. De modo que el proceso de implementación, las prácticas recomendadas para la política de protección frente a malware, etc., son las mismas que para el centro de datos y para cualquier otra área de la red.

Creación de reglas de bloqueo de tráfico en el centro de datos

Antes de crear reglas de aplicaciones permitidas para los cuatro flujos de tráfico del centro de datos, cree reglas de bloqueo y registro para bloquear aplicaciones que no use en el centro de datos, bloquear aplicaciones conocidas defectuosas y descubrir aplicaciones que pueda no saber que se encuentran en su red. El registro del tráfico bloqueado ofrece información sobre los posibles ataques para permitirte investigarlos.

Cuando descubra aplicaciones desconocidas, decida si debe permitirlas o si representan una amenaza potencial. Si estas reglas descubren aplicaciones que se deberían permitir, ajuste las reglas de aplicaciones permitidas en consecuencia. Si estas reglas descubren aplicaciones que no son legítimas, es posible que representen posibles amenazas y puede investigarlas usando la información de registro. No aplique perfiles de seguridad a las reglas de bloqueo porque el tráfico que controlan nunca accede a la red.

Si descubre aplicaciones desconocidas que son aplicaciones exclusivas internas u otros tipos de aplicaciones legítimas, cree una aplicación personalizada para cada aplicación desconocida, de modo que pueda identificarla y aplicarle una política de seguridad.

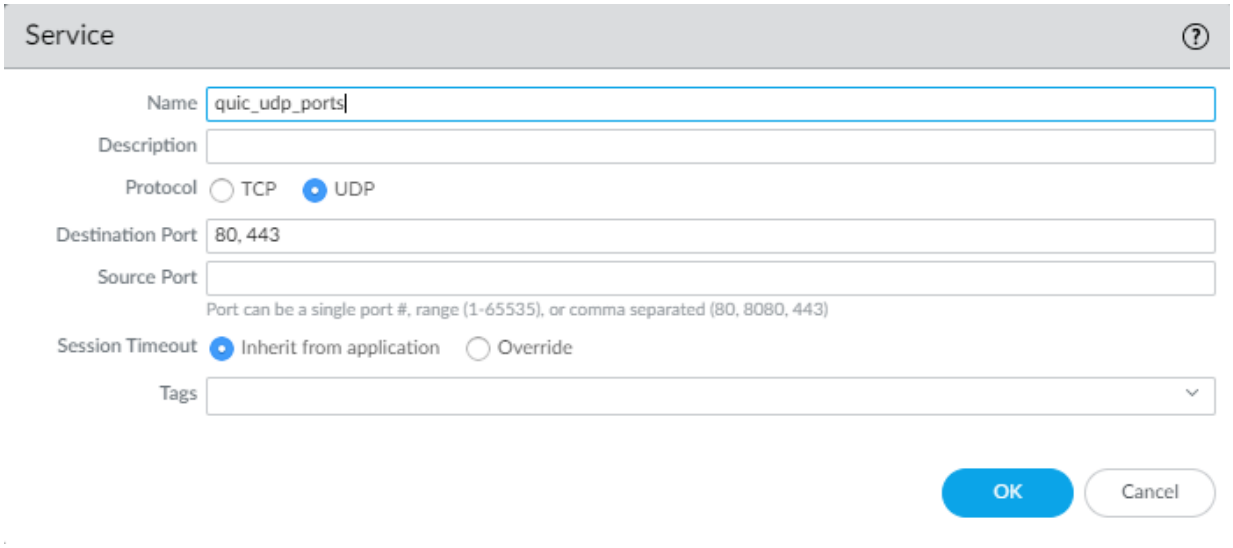
Orden de la base de reglas de la política de seguridad del centro de datos le muestra cómo ordenar estas reglas con todas las otras reglas que creamos para los cuatro flujos de tráfico en el centro de datos, de modo que ninguna regla enmascare a otra.

Para aplicar una política de seguridad uniforme en varios centros de datos, puede reusar las plantillas y las pilas de plantillas, de modo que las mismas políticas se apliquen en cada centro de datos. Las plantillas usan variables para aplicar valores para dispositivos específicos como direcciones IP, FQDN, etc., conservar una política de seguridad global y reducir el número de plantillas y pilas de plantillas que debe gestionar.

STEP 1 | Bloquee el protocolo de Conexiones UDP rápidas en Internet (QUIC).

Chrome y algunos otros exploradores establecen sesiones con QUIC en lugar de TLS, pero QUIC usa cifrado de propiedad que el cortafuegos no puede descifrar, por lo que tráfico potencialmente peligroso puede entrar en la red como tráfico cifrado. Bloquear QUIC obliga al explorador a volver a TLS y permite que el cortafuegos descifre el tráfico.

Cree una regla de políticas de seguridad para bloquear QUIC en sus puertos de servicio UDP (80 y 443) y cree una regla independiente para bloquear la aplicación QUIC. Para la regla que bloquea los puertos UDP 80 y 443, cree un servicio [**Objects (Objetos)** > **Services (Servicios)**] que incluya los puertos UDP 80 y 443:



Utilice el servicio para especificar los puertos UDP que se bloquearán para QUIC. En la segunda regla, bloquee la aplicación QUIC para que las dos primeras reglas de su base de reglas bloqueen QUIC:

	NAME	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
1	Block QUIC UDP	universal	l3-vlan-trust	any	any	any	l3-untrust	any	any	any	quic_udp_ports	Deny	none	
2	Block QUIC	universal	l3-vlan-trust	any	any	any	l3-untrust	any	any	quic	application-default	Deny	none	

STEP 2 | Bloquee todas las aplicaciones de zonas de usuario en el puerto application-default (aplicación-predeterminado) para identificar aplicaciones inesperadas.

Esta regla descubre aplicaciones que los usuarios intentar usar y que no sabía que se ejecutaban en su centro de datos. Supervise el tráfico que coincida con esta regla para determinar si representa una posible amenaza o si debe modificar las reglas de permiso para habilitar el acceso a la aplicación. Asegúrese de ubicar esta regla *después* de las reglas que permiten el tráfico o esta regla bloqueará el tráfico que desea permitir.

La regla que se muestra después de esta regla es similar a esta regla, a excepción de que se aplica al tráfico de cualquier origen, no solo tráfico de zonas de usuario. El motivo para crear reglas independientes es que es posible que los incumplimientos de la regla user-zone indiquen que está bloqueando una aplicación legítima que algunos usuarios requieren para hacer negocios, de modo que es posible que deba modificar una regla de permitidas para permitir la aplicación para un conjunto determinado de usuarios. Los incumplimientos en zonas que no sean de usuarios pueden indicar un cambio en una aplicación o un posible ataque. Crear una regla diferente para el resto del tráfico permite ver logs diferentes del tráfico de usuario y del resto del tráfico que intenta acceder al centro de datos, lo que facilita la investigación y la respuesta ante posibles problemas.

Esta regla debe estar antes de la próxima regla, que se aplica a todo el tráfico que puede registrar y supervisa los intentos de usar aplicaciones inesperadas en puertos application-default independientemente del origen después del primer incumplimiento al registro desde las zonas de usuario.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Unexpected-App-from-User-Zone	User to DC BP	universal	Contractors Engineering-Users Finance-Users IT-Users	any	any	any	Web-Server-Tier-DC	any	any	any	application-default	Drop	none	

Para crear esta regla:

- La Zona de origen incluye todas las zonas de usuario y los usuarios (su implementación puede tener más zonas de usuario que las que se muestran en el ejemplo).
- La Destination Zone (Zona de destino) es el nivel de servidor web del centro de datos (**Web-Server-Tier-DC**) en el perímetro del centro de datos.
- Configure la Application (Aplicación) como **any (cualquiera)** y el Service (Servicio) como **application-default**, de modo que la regla se aplique a todas las aplicaciones que se ejecuten en puertos estándar.
- Configure la Action (Acción) en **Drop (Descartar)** para descartar silenciosamente el tráfico sin enviar una señal al cliente o al servidor.

STEP 3 | Bloquee todas las aplicaciones de las zonas de usuario en cualquier puerto para identificar las aplicaciones que se ejecutan donde no deberían hacerlo.

Esta regla identifica aplicaciones conocidas y legítimas que los usuarios intentan ejecutar en puertos no estándar, así como aplicaciones desconocidas para las que es posible que deba crear aplicaciones personalizadas. Investigue el origen del tráfico que coincide con esta regla para garantizar que no permite tráfico unknown-tcp, unknown-udp o non-syn-tcp. Asegúrese de ubicar esta regla *después* de las reglas que permiten el tráfico o esta regla bloqueará el tráfico que desea permitir.

Además, se creará una regla de bloqueo diferente más adelante en esta sección que es similar a esta regla (Unexpected-App-from-Any-Zone), a excepción de que se aplica al tráfico de cualquier origen, no solo tráfico de zonas de usuario. El motivo para crear reglas diferentes es que es posible que los incumplimientos de la regla user-zone indiquen que una aplicación legítima que requieren algunos usuarios para hacer negocios no se diseñó correctamente, de modo que es posible que deba modificarla. Crear una regla diferente para el resto del tráfico permite ver logs diferentes del tráfico de usuario y del resto del tráfico que intenta acceder al centro de datos, lo que facilita la investigación y la respuesta ante posibles problemas.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Unexpected-User-App-Any-Port	User to DC BP	universal	Contractors Engineering-Users Finance-Users IT-Users	any	any	any	Web-Server-Tier-DC	any	any	any	any	Drop	none	

Para crear esta regla:

- La Zona de origen incluye todas las zonas de usuario y los usuarios (su implementación puede tener más zonas de usuario que las que se muestran en el ejemplo).
- La Destination Zone (Zona de destino) es el nivel de servidor web del centro de datos (**Web-Server-Tier-DC**) en el perímetro del centro de datos.
- Configure la Application (Aplicación) como **any (cualquiera)** y el Service (Servicio) como **any (cualquiera)**, de modo que la regla se aplique a todas las aplicaciones que se ejecuten en cualquier puerto.
- Configure la Action (Acción) en **Drop (Descartar)** para descartar silenciosamente el tráfico sin enviar una señal al cliente o al servidor.

STEP 4 | Bloquee aplicaciones diseñadas para evadir o sortear la seguridad, que los atacantes aprovechan o que no son necesarias en el centro de datos.

Esta regla protege al centro de datos de aplicaciones que no desea en su red. A pesar de que el objetivo de la política de seguridad recomendada es la aplicación positiva mediante el uso de reglas de aplicaciones permitidas, bloquear y generar logs de manera explícita sobre la actividad de aplicaciones peligrosas, como aplicaciones de uso compartido de archivos no sancionadas, aplicaciones de acceso remoto o túneles cifrados, brinda visibilidad e información sobre posibles ataques. Incluso tras desarrollar una lista de aplicaciones permitidas sólida, conserve esta regla de bloqueo de aplicaciones en la base de reglas debido a que los logs de posibles incumplimientos ayudan a investigar posibles ataques.

Use esta regla para bloquear solo las aplicaciones que no desea en su centro de datos.

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Block-Bad-Apps	User to DC BP	universal	any	any	any	any	App-Server-Tier-DC DB-Server-Tier-DC Engineering-DC-Infra Finance-DC-Infra IT Infrastructure SAP-Infra Web-Server-Tier-DC	any	any	Encrypted-Tunnels File-Sharing Remote-Access	any	Drop	none	

Para crear esta regla:

- Configure Source Zone (Zona de origen), Address (Dirección), User (Usuario) y Device (Dispositivo) en **any (cualquiera)** debido a que bloquea aplicaciones que nadie debería poder usar en el centro de datos.
- Especifique todas las zonas del centro de datos en Destination Zone (Zona de destino) para proteger a todos los servidores del centro de datos de las aplicaciones malintencionadas.
- Cree un filtro de aplicación para cada tipo (categoría) de aplicación que desee bloquear y especifique las aplicaciones adicionales. En este ejemplo, se incluyen filtros de aplicaciones para túneles cifrados, acceso remoto y uso compartido de archivos. Bloquee las aplicaciones que no usa en el centro de datos para reducir la superficie de ataque al eliminar las aplicaciones innecesarias, lo que también reduce el riesgo. La ventaja de usar filtros de aplicación en lugar de grupos de aplicaciones individuales es que los filtros se actualizan automáticamente, de modo que no debe realizar mantenimiento cuando aparecen nuevas aplicaciones.
- Configure Service (Servicio) en **any (cualquiera)** para capturar las aplicaciones no deseadas en los puertos no estándar y los puertos predeterminados.
- Configure la Action (Acción) en **Drop (Descartar)** para descartar silenciosamente el tráfico sin enviar una señal al cliente o al servidor.

Los filtros de aplicación que se muestran en el ejemplo de regla no forman una lista completa. Evalúe la lista de aplicaciones que creó en función de la evaluación del centro de datos y añada las aplicaciones que no desea permitir a esta regla. Ubique esta regla de bloqueo *después* de la regla de permitidos para permitir excepciones a la regla. Por ejemplo, el departamento de TI necesita usar aplicaciones de acceso remoto para gestionar los dispositivos del centro de datos, de modo que debe permitir el uso de las aplicaciones de acceso remoto antes de bloquearlas para el resto de los usuarios. Otro ejemplo es que puede autorizar una o más aplicaciones de uso compartido de archivos en las reglas de permitidos anteriores a esta regla de bloqueo, y el filtro de aplicaciones en esta regla bloqueará el resto de estas aplicaciones. Si existen conjuntos de aplicaciones o aplicaciones individuales que no desea en la red y para las que no hay excepciones, puede crear una regla de bloqueo específica para bloquear esas aplicaciones y ubicarla en la parte superior de la base de reglas, por encima de las reglas de aplicaciones

permitidas. Sin embargo, si hace esto, debe estar seguro de que ninguna de las aplicaciones bloqueadas tenga usos comerciales legítimos porque sus usuarios no podrán acceder a ellas.

STEP 5 | Bloquee todas las aplicaciones de cualquier zona en el puerto application-default para identificar aplicaciones inesperadas.

Esta regla descubre aplicaciones de cualquier zona que no sabía que se ejecutaban en su centro de datos. Los incumplimientos a esta regla pueden indicar que una aplicación cambió o pueden indicar una posible amenaza. Supervise el tráfico que coincida con esta regla para determinar si supone una posible amenaza o si debe modificar las reglas de aplicaciones permitidas. Asegúrese de ubicar esta regla *después* de reglas que permiten tráfico o esta regla bloqueará el tráfico que intenta permitir, y después de la regla en el paso 1, de modo que no capture tráfico de zonas de usuario.

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-from-Any-Zone	universal	any	any	any	any	Web-Server-Tier-DC	any	any	any	application-default	Drop	none	

Para crear esta regla:

- Source (Origen) es **any (cualquiera)** para abarcar el resto del tráfico que intente acceder al centro de datos (la regla en el paso 1 bloquea e identifica las aplicaciones de usuarios inesperados antes de que el tráfico coincida con esta regla).
- La Destination Zone (Zona de destino) es el nivel de servidor web del centro de datos (**Web-Server-Tier-DC**) en el perímetro del centro de datos.
- Configure la Application (Aplicación) como **any (cualquiera)** y el Service (Servicio) como **application-default**, de modo que la regla se aplique a todas las aplicaciones que se ejecuten en puertos estándar.
- Configure la Action (Acción) en **Drop (Descartar)** para descartar silenciosamente el tráfico sin enviar una señal al cliente o al servidor.

STEP 6 | Bloquee todas las aplicaciones de cualquier zona en cualquier puerto para identificar las aplicaciones que se ejecutan donde no deberían hacerlo.

Esta regla identifica aplicaciones conocidas y legítimas que intentan ejecutarse en puertos no estándar, así como aplicaciones desconocidas para las que es posible que deba crear aplicaciones personalizadas. Investigue el origen del tráfico que coincide con esta regla para garantizar que no permite tráfico unknown-tcp, unknown-udp o non-syn-tcp. Asegúrese de ubicar esta regla *después* de las reglas que permiten tráfico o esta regla bloqueará el tráfico que intenta permitir, y después de la regla anterior, de modo que no capture tráfico de zonas de usuario.

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-Any-Port	universal	any	any	any	any	Web-Server-Tier-DC	any	any	any	any	Drop	none	

Para crear esta regla, use los mismos ajustes que en la regla **Unexpected-App-from-User-Zone**, pero en lugar de especificar las zonas de usuario en el origen, especifique **any (cualquiera)** en el tipo de zona que abarcará el resto del tráfico que intente acceder al centro de datos y configure Service (Servicio) como **any (cualquiera)** para que abarque puertos no estándar.

STEP 7 | Descubra usuarios desconocidos que intenten ejecutar cualquier aplicación en cualquier puerto.

Esta regla identifica brechas en la cobertura de User-ID hallando usuarios desconocidos. Además, identifica dispositivos en riesgo o integrados en la comunidad del usuario que intentan acceder al centro de datos. (Los dispositivos integrados no poseen interfaz de usuario, como las impresoras, los lectores de tarjetas y las cámaras, pero los adversarios pueden poner estos dispositivos en riesgo y usarlos en un ataque).

NAME	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
		ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Discover-Unknown-Users	universal	any	any	unknown	any	any	any	any	any	any	Deny	none	

Esta regla es muy similar a la regla interzone-default (interzona-predeterminada) que evita la comunicación entre zonas (a menos que otra regla permita el tráfico), pero en lugar de eliminar el tráfico de todos los usuarios, solo elimina el tráfico de usuarios desconocidos. Esto le permite registrar las coincidencias de la regla de manera separada e investigar con mayor facilidad a los usuarios desconocidos que intentan acceder al centro de datos.

Definición de la política de seguridad para el tráfico inicial desde el usuario hacia el centro de datos

La definición de las políticas de seguridad iniciales recomendadas para el tráfico de usuario que fluye hacia el centro de datos inicia el proceso de desarrollo de una lista de aplicaciones permitidas para el centro de datos. El principal objetivo es usar la aplicación positiva de la seguridad para proteger el centro de datos con una arquitectura de confianza cero controlando explícitamente quién puede acceder al centro de datos, a qué aplicaciones en el centro de datos pueden acceder y a qué recursos pueden acceder en el centro de datos. Cuando termine de desarrollar la política de seguridad recomendada, los usuarios desconocidos no deberían poder acceder al centro de datos y las aplicaciones o recursos desconocidos no deberían poder residir en el centro de datos.

- Enfoques hacia la seguridad del tráfico desde el usuario hacia el centro de datos
- Creación de reglas de aplicaciones permitidas desde el usuario al centro de datos
- Creación de reglas para la política de autenticación desde el usuario hacia el centro de datos
- Creación de reglas para la política de descifrado desde el usuario hacia el centro de datos

Enfoques hacia la seguridad del tráfico desde el usuario hacia el centro de datos

El enfoque heredado tradicional de proteger el tráfico de usuario que fluye hacia el centro de datos expone activos valiosos al riesgo, mientras que el enfoque recomendado protege sus activos valiosos.

El enfoque tradicional	Riesgo	El enfoque recomendado
Las reglas basadas en el puerto brindan suficiente seguridad debido a que el centro de datos se encuentra dentro de una red fiable.	Las aplicaciones malintencionadas acceden a la red falsificando números de puertos, creando túneles en un puerto o usando saltos de puertos para evitar la detección.	Las reglas de aplicaciones permitidas aúnan aplicaciones, usuarios y servidores, de modo que solo los usuarios legítimos que usen aplicaciones sancionadas puedan acceder a los conjuntos adecuados de servidores del centro de datos. *Cuando pase de reglas basadas en el puerto a reglas basadas en la aplicación, en la base de reglas, ubique la regla basada en la aplicación sobre la regla basada en el puerto que reemplazará. Restablezca el contador de coincidencias de la regla de la política de ambas reglas. Si el tráfico coincide con la regla basada en el puerto, el conteo de coincidencias de la regla de la política aumenta.*

El enfoque tradicional	Riesgo	El enfoque recomendado
		Ajuste la regla basada en la aplicación hasta que no existan coincidencias entre el tráfico y la regla basada en el puerto durante un tiempo, y elimine la regla basada en el puerto.
Confíe en los usuarios internos y permita que la aplicación a la que acceda el usuario determine si permite el acceso en función de credenciales y reglas de direcciones IP.	Un atacante obtiene acceso a un endpoint del centro de datos y se mueve lateralmente a otro endpoint del centro de datos para aprovechar credenciales robadas o vulnerabilidades en el lado del servidor. Los usuarios desconocidos obtienen acceso a los endpoints del centro de datos.	Habilite User-ID, bloquee usuarios desconocidos y permita el acceso a usuarios autorizados. Cree dominios de identidad diferentes para empleados, socios y contratistas. Use autenticación multifactor (multi-factor authentication, MFA) para socios, contratistas y el acceso a servidores confidenciales.
Analizar archivos desconocidos es innecesario debido a que el centro de datos se encuentra en una red fiable.	Es posible que los usuarios descarguen malware accidentalmente desde aplicaciones de uso compartido de archivos u otras aplicaciones de la nube.	Envíe todos los archivos desconocidos a WildFire para analizarlos e identificar malware nuevo y desconocido, y protegerse contra ello.
Una combinación de perfiles de prevención de amenazas de varios proveedores.	Un conjunto de herramientas individuales ofrece brechas de seguridad a los atacantes y es posible que no funcionen adecuadamente.	El conjunto de herramientas de seguridad coordinada de Palo Alto Networks trabaja en conjunto para encender la seguridad y evitar ataques.

Creación de reglas de aplicaciones permitidas desde el usuario al centro de datos

Cuando evalúa el centro de datos, obtiene la información para crear un conjunto de reglas de aplicaciones permitidas en función de decisiones determinadas sobre quién debe poder acceder a cada aplicación que se ejecuta en cada conjunto de servidores. Cree las reglas de aplicaciones permitidas de la política de seguridad [**Policies (Políticas)** > **Security (Seguridad)**], de modo que únicamente los usuarios que permita explícitamente puedan usar las aplicaciones que pertenecen a su trabajo solo en los conjuntos adecuados de servidores. No permita accesos innecesarios, usuarios desconocidos ni aplicaciones desconocidas.

Etiquete todas las aplicaciones sancionadas *con la etiqueta Sanctioned (Sancionado) predefinida. Panorama y los cortafuegos consideran a las aplicaciones sin la etiqueta Sanctioned (Sancionado) como aplicaciones no sancionadas.*

Orden de la base de reglas de la política de seguridad del centro de datos le muestra cómo ordenar estas reglas con todas las otras reglas que creamos para los otros tres flujos de tráfico en el centro de datos y las reglas de bloqueo, de modo que ninguna regla enmascareque a otra.

Para aplicar una política de seguridad uniforme en varios centros de datos, puede reusar las plantillas y las pilas de plantillas, de modo que las mismas políticas se apliquen en cada centro de datos. Las plantillas usan variables para aplicar valores para dispositivos específicos como direcciones IP, FQDN, etc., conservar una política de seguridad global y reducir el número de plantillas y pilas de plantillas que debe gestionar.

Cada una de las siguientes reglas de permiso:

- Tiene la práctica recomendada grupo de perfiles de seguridad adjunta, que consta de los perfiles de seguridad de práctica recomendada. El uso de un grupo de perfiles de seguridad le permite aplicar todos los perfiles de prácticas recomendadas a una regla a la vez en lugar de especificar cada perfil individualmente. Los grupos de perfiles de seguridad hacen que la configuración de la protección contra malware, vulnerabilidades, tráfico C2 y amenazas conocidas y desconocidas sea más rápida y sencilla.
- Registra el tráfico (al final de la sesión) para que pueda realizar un seguimiento y analizar las infracciones de las reglas, e incluye el reenvío de logs. Reenvíe los logs a los servidores de logs y, cuando corresponda, reenvíe los correos electrónicos de logs a los administradores correspondientes.

STEP 1 | Habilite el acceso del usuario adecuado a los servidores DNS corporativos internos (no permita el acceso a los servidores DNS externos).

Esta regla limita el acceso a los servidores DNS corporativos, lo que reduce la superficie de ataque y permite proteger las entradas DNS sobre hosts y servicios internos. Para evitar que las solicitudes DNS públicas las descubran, las entradas DNS de los recursos corporativos internos no se almacenan en servidores DNS públicos. Por lo tanto, la única manera en la que un atacante puede descubrir estas entradas es poner un servidor DNS corporativo en riesgo, de modo que sus servidores DNS son objetivos atractivos.

En la puerta de enlace de internet (perímetro de la red), bloquee todo el tráfico DNS hacia servidores DNS públicos. No permita que el tráfico DNS se dirija a internet.

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
DNS Services	User to DC BP	universal	any	any	any	any	IT Infrastructure	DNS-Servers	any	dns	application-default	Allow		

Esta regla es una excepción a la práctica recomendada de no permitir a "ningún" usuario en las reglas de la política debido a que los usuarios requieren acceso a los servicios DNS antes de iniciar sesión. Esta regla protege el acceso a los servicios DNS. Para crear esta regla:

- Limite el acceso a la zona de destino adecuada en el centro de datos, **IT infrastructure (Infraestructura de TI)**.
- Configure un grupo de direcciones para los **DNS Servers (Servidores DNS)** y limite el acceso a solo ese grupo.
- Evite el acceso usando cualquier aplicación excepto **dns**.
- Es especialmente importante aplicar el grupo de perfiles de seguridad de prácticas recomendadas al tráfico de DNS porque si un atacante secuestra su servidor DNS, el atacante puede redirigir el tráfico a sitios web de phishing que se parecen a los sitios web legítimos a los que los usuarios intentan acceder.

STEP 2 | Brinde acceso privilegiado al personal de TI protegido necesario a los servidores del centro de datos para gestión y mantenimiento.

Esta regla muestra cómo proteger el acceso a sistemas críticos para los usuarios con cuentas privilegiadas. Las cuentas privilegiadas requieren un nivel elevado de confianza y conceden acceso administrativo a sistemas críticos que contienen los datos más valiosos de la empresa, de modo que debe controlar y supervisar las cuentas privilegiadas con mayor rigor. Aproveche App-ID para especificar únicamente las aplicaciones que necesitan los usuarios de TI para gestionar dispositivos del centro de datos, de modo que el cortafuegos bloquee el acceso del resto de las aplicaciones. En este ejemplo, un grupo de usuarios de TI requiere acceso administrativo para gestionar servidores del centro de datos.

El acceso privilegiado del departamento de TI para la gestión del servidor del centro de datos debe limitarse a las interfaces de gestión y debe encontrarse en una VLAN exclusiva, de modo que el tráfico de gestión del servidor esté separado de otro tráfico. Las interfaces de gestión deben estar en la misma subred. No permita este tipo de acceso en interfaces de datos. Si el grupo de TI usa SSH o RDP para el acceso de gestión, no permita el acceso de SSH o RDP con otros fines.

La organización de su equipo de redes de TI determina a quién se le concede acceso privilegiado de TI. Para cada tipo de acceso privilegiado, agrupe los servidores y otros dispositivos por sus requisitos de acceso. Permita únicamente que los usuarios de TI necesarios accedan a cada conjunto de servidores, usando únicamente las aplicaciones necesarias para la gestión de dispositivos.

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
IT DC Server Management	User to DC BP	universal	IT-Users	any	it-superusers	any	IT-Server-Access-DC	IT-Server-Management	any	ms-rdp ssh ssl	Custom-IT-Ports	Allow		

Para crear esta regla:

- Debido a que solo un subconjunto de usuarios de TI puede gestionar los servidores del centro de datos, aproveche User-ID para crear un grupo específicamente para los usuarios de TI que requieren ese nivel de acceso privilegiado (en este ejemplo, **it-superusers**).
- Cree un grupo de direcciones dinámicas (**IT-Server-Management**) con las direcciones de la interfaz de gestión de los servidores que desea que **it-superusers** gestione y limite Destination (Destino) a ese grupo de direcciones en la zona **IT-server-access-DC**.
- Permita únicamente las aplicaciones que los superusuarios de TI necesitan para realizar sus tareas empresariales en los puertos predeterminados. En este ejemplo, la regla permite las aplicaciones **ssl**, **ssh** y **ms-rdp**.

Las aplicaciones permitidas son ejemplos. Permita las aplicaciones que el departamento de TI use para gestionar los servidores en el centro de datos. En algunos casos, es posible que las aplicaciones en SSL requieran que se incorpore la aplicación específica para que se puedan identificar correctamente por App-ID.

El personal de TI también gestiona conmutadores, enrutadores y otros dispositivos en el centro de datos. Si el mismo grupo de usuarios de TI gestiona esos recursos usando las mismas aplicaciones, puede añadirlos a la zona y dirección de destino, de modo que la regla permita a los superusuarios de TI acceder a las interfaces de gestión de esos dispositivos. Si diferentes grupos de usuarios de TI gestionan diferentes conjuntos de recursos del centro de datos o usan diferentes aplicaciones, cree reglas estrictas y separadas en la política de seguridad para cada grupo de usuarios y cada conjunto de aplicaciones.

Debido a que los grupos de usuarios con cuentas privilegiadas cuentan con acceso a sistemas críticos, cuando cree reglas para la política de autenticación desde el usuario hacia el centro de datos, requiera MFA para evitar el acceso si los atacantes ponen las credenciales en riesgo. Cree las reglas correspondientes en la política de autenticación y la política de descifrado para cada regla de acceso privilegiado.

STEP 3 | Permita el acceso a los grupos de usuarios empleados con motivos empresariales legítimos para comunicarse con los servidores del centro de datos.

Esta regla muestra cómo limitar el acceso de cada grupo de usuarios (o, en algunos casos, un usuario) a únicamente las aplicaciones y los servidores necesarios. Por ejemplo, los ingenieros deben acceden a servidores de desarrollo en el centro de datos. Para crear una regla en la política de seguridad, cree un grupo de direcciones dinámicas con las direcciones IP de todos los servidores de desarrollo del centro de datos que usa el grupo, identifique las aplicaciones que necesitan usar los ingenieros en esos servidores y cree la regla en función de esos grupos.

			Source				Destination								
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Engineering Resources	User to DC BP	universal	Engineering-Users	any	api-users engg-users	any	Engineering-DC-Infra	Dev-Servers	any	oracle-bi perforce profinet qlikview	application-default	Allow		

Para crear esta regla:

- Especifique los grupos de usuarios de ingeniería que requieren acceso a los servidores de ingeniería en el centro de datos, en este ejemplo, **api-users** y **engg-users**.
- Limite el acceso a los servidores de desarrollo del centro de datos creando un grupo de direcciones dinámicas (**Dev-Servers**) para ellos y estableciéndolo como Destination Address (Dirección de destino).
- Limite el acceso únicamente a las aplicaciones necesarias por motivos empresariales en los puertos predeterminados.

Use el mismo método para crear reglas de permiso detalladas para cada grupo de usuarios (de ser necesario, también puede hacerlo para usuarios individuales), de modo que cada grupo use únicamente las aplicaciones legítimas que se ejecutan en puertos predeterminados para acceder a los conjuntos de servidores a los que acceden por motivos empresariales. Por ejemplo, permita únicamente el grupo de usuarios de finanzas que deben poder acceder a los servidores que contienen PCI para acceder a estos servidores usando únicamente las aplicaciones de finanzas sancionadas necesarias para realizar los objetivos del negocio.

			Source				Destination								
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Finance to DC	User to DC BP	universal	Finance-Users	any	accounting-users finance-users	any	Finance-DC-Infra	Fin-Servers	any	netsuite oracle oracle-crm-ondemand oracle-forms	application-default	Allow		

De manera similar a la regla de permitidos para el acceso de usuarios de ingeniería a los servidores del centro de datos, esta regla permite a los usuarios en los grupos **finance-users** y **accounting-users** usar únicamente las aplicaciones especificadas para acceder a los servidores en el grupo de direcciones dinámicas **Fin-Servers**. La regla aplica los perfiles de seguridad recomendados al tráfico permitido y registra la actividad.

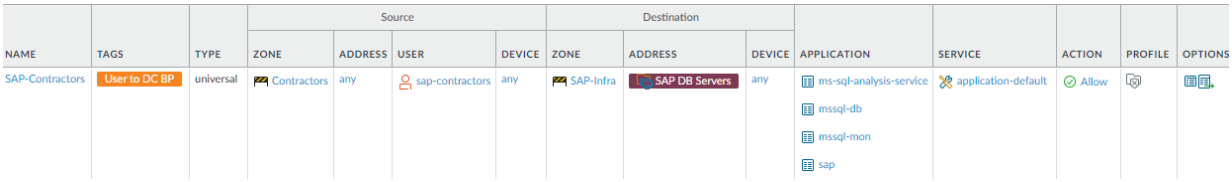
STEP 4 | Permita acceso limitado y específico al centro de datos a contratistas, socios, clientes y terceros.

Esta regla muestra cómo controlar estrictamente el acceso de usuarios externos, de modo que puedan usar únicamente las aplicaciones que necesitan solo en los servidores que necesitan. Por ejemplo, una empresa contrata un grupo de contratistas desarrolladores de SAP. Los desarrolladores de SAP necesitan acceder a la base de datos de SAP en el centro de datos y realizan consultas de SQL. Sin embargo, SQL también se ejecuta en bases de datos de producción a las que los desarrolladores de SAP no deben acceder. La empresa debe controlar tres vectores de acceso:

- **Grupo de usuarios:** contratistas desarrolladores de SAP.
- **Aplicaciones:** MS-SQL y SAP.

- **Servidores:** únicamente los servidores de bases de datos de SAP. Bloquee el resto del acceso al servidor del centro de datos.

La combinación de User-ID para aislar el grupo de usuarios contratistas de SAP, App-ID para limitar el grupo a usar únicamente las aplicaciones necesarias y un grupo de direcciones dinámicas que limite el acceso a únicamente los servidores de la base de datos de SAP en el centro de datos permite a la empresa brindar exactamente el acceso que los contratistas de SAP necesitan para realizar sus tareas y nada más.



Para crear esta regla:

- Especifique Source Zone (Zona de origen) y User (Usuario) para limitar el acceso de los usuarios del grupo **sap-contractors** proveniente de la zona **Contractors (Contratistas)**.
- Limite Destination (Destino) a los servidores de la base de datos de SAP (grupo de direcciones dinámicas **SAP DB Server**) en la zona **SAP-Infra**.
- Permita a los contratistas de SAP usar únicamente las aplicaciones que necesitan para realizar sus tareas empresariales en los puertos predeterminados. En este ejemplo, la regla permite las aplicaciones **ms-sql-analysis-service**, **mssql-db**, **mssql-mon** y **sap**.

Las reglas de permiso detalladas de la política de seguridad evitan todo el acceso menos el que se requiere por motivos empresariales y reducen el riesgo reduciendo la superficie de ataque. Cree reglas de permiso similares para cada grupo externo que requiera acceso al centro de datos.

En lugar de confiar en que los usuarios y las empresas externas protegen sus credenciales, requiera autenticación multifactor (multi-factor authentication, MFA) (Creación de reglas para la política de autenticación desde el usuario hacia el centro de datos) para evitar el acceso si los atacantes roban credenciales o ponen a los sistemas externos en riesgo de otra manera. La autenticación con MFA habría evitado numerosas filtraciones de alto perfil exitosas en los últimos años.

Verifique que solo se ejecuten las aplicaciones que tienen permiso explícito en las reglas de la política de seguridad viendo el informe de aplicaciones predefinido (**Monitor [Supervisar]** > **Reports [Informes]** > **Application Reports [Informes de aplicación]** > **Applications [Aplicaciones]**). Si ve aplicaciones inesperadas en el informe, revise las reglas de aplicaciones permitidas y vuelva a ajustarlas, de modo que no permitan aplicaciones inesperadas.

Creación de reglas para la política de autenticación desde el usuario hacia el centro de datos

Las reglas en la política de autenticación obligan a los usuarios a probar que son quienes dicen ser antes de que puedan acceder a los servicios, aplicaciones y otros recursos del centro de datos. La autenticación es especialmente importante durante la protección de sus activos más valiosos debido a que si el atacante borra credenciales y se autentica ante el cortafuegos, es posible que el atacante acceda y ponga a los activos en el centro de datos en riesgo.

Para acceder a servidores confidenciales y brindar acceso a usuarios externos a los servidores (por ejemplo, los contratistas de desarrollo de SAP que acceden a servidores de SAP en el centro de datos), implemente autenticación multifactor (Multi-Factor Authentication, MFA) para evitar que los atacantes usen credenciales robadas para acceder a esos sistemas. Una política de autenticación con MFA habría evitado numerosas filtraciones de alto perfil exitosas en los últimos años.

Antes de crear reglas en la política de autenticación (**Policies [Políticas]** > **Authentication [Autenticación]**), debe configurar las dependencias de la política de autenticación para unir el método de autenticación, el tipo de autenticación, cómo acceder al servidor de autenticación y el uso del portal de autenticación para una regla de política de autenticación que especifique quién puede autenticarse en cada servidor con qué servicios.

STEP 1 | Autentique grupos de usuarios empleados y personas que tengan motivos empresariales legítimos para usar servidores del centro de usuario.

Esta regla muestra cómo autenticar grupos de usuarios, de modo que puedan acceder a los servicios que requieren sus actividades comerciales en los servidores necesarios. Por ejemplo, los ingenieros deben autenticarse antes de poder acceder a los servidores y aplicaciones de desarrollo.

		Source				Destination					
NAME	TAGS	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	SERVICE	AUTHENTICATION ENFORCEMENT	LOG SETTINGS
DevEng Resources	User to DC BP	Engineering-Users	any	api-users engg-users	any	Engineering-DC-Infra	Dev-Servers	any	Perforce rdp service-http service-https ssh	Auth-Dev-Servers	Log Authentication Timeouts: yes Log Forwarding: Auth-LF

Para crear esta regla:

- Especifique los grupos de usuarios de ingeniería que deben autenticarse antes de que puedan acceder a los servidores de ingeniería, en este ejemplo, **api-users** y **engg-users**.
- Aplique autenticación a estos grupos de usuarios para las solicitudes de acceso al servidor de desarrollo del centro de datos creando un grupo de direcciones dinámicas (**Dev-Servers**) para ellos y estableciéndolo como la dirección de destino.
- Aplique la regla de autenticación a los servicios que los grupos de ingeniería necesitan usar por motivos empresariales, en este ejemplo, **Perforce**, **rdp**, **service-http**, **service-https** y **ssh** (es posible que los desarrolladores necesiten usar SSH y RDP para acceder a los servidores Linux y deban autenticarse antes de poder acceder a los servidores). Los servicios en las reglas de autenticación dependen de los servicios que necesitan usar los grupos.
- Configure un objeto de aplicación de autenticación (**Auth-Dev-Servers**) que especifique el método de autenticación y el perfil de autenticación, y añádalo a la regla.
- Registre la actividad, de modo que pueda realizar un seguimiento y analizar los incumplimientos de la regla, lo que puede indicar un posible ataque.

Otro caso de uso de la autenticación es cuando un grupo requiere acceso a un conjunto determinado de servicios. Por ejemplo, los usuarios del departamento de finanzas necesitan acceder a información de la tarjeta de pago (Payment Card Information, PCI) confidencial usando servicios específicos y deben autenticarse antes de poder acceder. Para autenticar usuarios para esos servicios, esta regla usa un grupo de servicio personalizado (**Objects [Objetos]** > **Service Groups [Grupos de servicio]**) que solo incluye los servicios para los que el cortafuegos debe autenticar a los usuarios de finanzas.

		Source				Destination					
NAME	TAGS	ZONE	ADDR...	USER	DEVI...	ZONE	ADDRESS	DEVI...	SERVICE	AUTHENTICATION ENFORCEMENT	LOG SETTINGS
Finance Servers	User to DC BP	Finance-Users	any	accounting-users finance-users	any	Finance-DC-Infra	Fin-Servers	any	Custom-Finance-Srvrs-Services service-http service-https	Auth-Finance-Servers	Log Authentication Timeouts: yes Log Forwarding: Auth-LF

Para crear esta regla:

- Especifique los grupos de usuarios que deben autenticarse antes de que puedan acceder a los servidores de finanzas en el centro de datos, en este ejemplo, **accounting-users** y **finance-users**.
- Aplique autenticación a estos grupos de usuarios para las solicitudes de acceso al servidor de finanzas del centro de datos creando un grupo de direcciones dinámicas (**Fin-Servers**) para ellos y estableciéndolo como la dirección de destino.

- Aplique la regla de autenticación a los servicios que los usuarios de finanzas deben usar por motivos empresariales, en este ejemplo, **service-http**, **service-https** y los servicios definidos en el grupo de servicios personalizado **Custom-Finance-Srvrs-Services**, de modo que los usuarios deban autenticarse antes de que puedan acceder a estos servicios.
- Configure un objeto de aplicación de autenticación (**Auth-Finance-Servers**) que especifique el método de autenticación y el perfil de autenticación, y añádalo a la regla.
- Registre la actividad, de modo que pueda realizar un seguimiento y analizar los incumplimientos de la regla, lo que puede indicar un posible ataque.

STEP 2 | Autentique a contratistas, socios, clientes y otros grupos de no empleados que requieran acceso al centro de datos.

Esta regla requiere MFA para los grupos de usuarios externos como contratistas, socios y clientes debido a que tiene menos control de las prácticas empresariales y de seguridad de sus empresas y su personal que el que tiene sobre sus empleados. Solicitar a estos usuarios que se autentiquen con al menos dos factores protege al centro de datos del robo de credenciales de una empresa externa.

		Source				Destination					
NAME	TAGS	ZONE	ADDR...	USER	DEVI...	ZONE	ADDRESS	DEVI...	SERVICE	AUTHENTICATI... ENFORCEMENT	LOG SETTINGS
SAP Resources	User to DC BP	Contractors	any	sap-contractors	any	SAP-Infra	SAP DB Servers	any	SAP-Services service-http service-https	Auth-SAP-Servers	Log Authentication Timeouts: yes Log Forwarding: Auth-LF

Para crear esta regla:

- Aplique la regla de autenticación a los servicios que deben usar los contratistas de SAP por motivos empresariales. Cree un grupo de servicio personalizado (**Sap-Services**) para definir los puertos en los que los contratistas de SAP pueden autenticarse y añadir los servicios necesarios, en este ejemplo, **service-http** y **service-https**.
- Configure un objeto de aplicación de autenticación (**Auth-SAP-Servers**) que especifique el método de autenticación y el perfil de autenticación, y añádalo a la regla. En este caso, el tipo de autenticación debe admitir MFA y debe **Add (Añadir)** un perfil de servidor de MFA al perfil de autenticación (pestaña **Factors [Factores]**), y debe realizar el resto de los pasos para configurar la MFA.

  Configure la MFA para autenticar a todos los usuarios y grupos de usuarios que acceden a sistemas confidenciales para protegerse de los atacantes con credenciales robadas.
- Registre la actividad, de modo que pueda realizar un seguimiento y analizar los incumplimientos de la regla, lo que puede indicar un posible ataque.

STEP 3 | Autentique usuarios que requieran acceso especializado, como el personal de TI que requiere acceso seguro a los servidores del centro de datos para realizar gestión y mantenimiento.

Esta regla muestra cómo configurar la autenticación para los usuarios con cuentas privilegiadas, que concede accesos administrativos a sistemas críticos. Debido a que poner en riesgo las credenciales de un usuario privilegiado permite que el atacante acceda al centro de datos y a los activos valiosos, debe protegerse de las credenciales robadas requiriendo al menos dos factores de autenticación para garantizar que solo se conceda acceso a los usuarios legítimos. En este ejemplo, se muestra cómo autenticar a los usuarios de TI correctos para acceder a las interfaces de gestión del servidor del centro de datos.

		Source				Destination					
NAME	TAGS	ZONE	ADDR...	USER	DEVI...	ZONE	ADDRESS	DEVI...	SERVICE	AUTHENTICATION ENFORCEMENT	LOG SETTINGS
IT Secured Access	User to DC BP	IT-Users	any	it-superusers	any	IT-Server-Access-DC	IT-Server-Management	any	Custom-IT-Ports	Auth-IT-Server-Mgmt	Log Authentication Timeouts: yes Log Forwarding: Auth-LF

Para crear esta regla:

- Especifique los usuarios de cuentas privilegiadas que deben autenticarse antes de poder acceder a las interfaces de gestión del servidor del centro de datos, en este ejemplo, el grupo **it-superusers**.
- Aplique autenticación al grupo de usuarios para las solicitudes de acceso a la interfaz de gestión del centro de datos creando un grupo de direcciones dinámicas (**IT-Server-Management**) para ellos y estableciéndolo como la dirección de destino.
- Aplique la regla de autenticación a los servicios que necesita usar el personal de TI privilegiado por motivos empresariales, en este ejemplo, el grupo de servicios personalizado **Custom-IT-Ports**, que identifica a todos los puertos de gestión del servidor (que deben ubicarse en la misma subred).
- Configure y aplique un objeto de aplicación de autenticación (**Auth-IT-Server-Mgmt** en este ejemplo) que aplique la MFA (dos factores) necesaria para la autenticación. Haga clic en **Add (Añadir)** para añadir un perfil de servidor de MFA al perfil de autenticación (pestaña **Factors [Factores]**) y realice el resto de los pasos para configurar la MFA. Usar la MFA es crítico debido a debe estar seguro de la identidad de cada usuario de TI con una cuenta privilegiada dado que cuentan con acceso a la gestión del dispositivo.

  Para reducir aún más la posibilidad de que un atacante ponga al centro de datos en riesgo usando credenciales robadas o aprovechando un momento oportuno cuando una estación de trabajo esté sin supervisión, pero no bloqueada, cuando configure la MFA, configure las marcas de tiempo de autenticación para los factores de autenticación. En el caso de los activos valiosos del centro de datos, se recomienda establecer prioridades protegiendo servicios y aplicaciones.
- Registre la actividad, de modo que pueda realizar un seguimiento y analizar los incumplimientos de la regla.

El personal de TI también gestiona conmutadores, enrutadores y otros dispositivos en el centro de datos. Si el mismo grupo de usuarios de TI gestiona esos recursos, puede añadirlos a la zona y dirección de destino, de modo que la regla autentique a los superusuarios de TI antes de que puedan acceder a las interfaces de gestión de esos dispositivos. Si diferentes usuarios de TI gestionan diferentes conjuntos de recursos del centro de datos, cree reglas estrictas diferentes en la política de seguridad y las reglas en la política de descifrado y la política de autenticación correspondientes a cada grupo de usuarios.

No envíe credenciales en texto no cifrado. Por ejemplo, si usa RADIUS, use un método de EAP compatible para transportar credenciales a TLS de manera segura.

Creación de reglas para la política de descifrado desde el usuario hacia el centro de datos

Cree reglas en la política de descifrado para el tráfico que accede al centro de datos desde la población de usuarios para proporcionar visibilidad, de modo que pueda inspeccionar el tráfico y proteger sus activos más valiosos. Cuando cree una regla en la política de seguridad que permite el acceso a un grupo de usuarios (o un usuario determinado) a un conjunto de servidores de centro de datos, cree una regla en la política de descifrado para descifrar el tráfico.

Debido a que el centro de datos aloja sus activos más valiosos, descifre todo el tráfico del centro de datos que pueda descifrar. Comience por descifrar el tráfico que se dirige a los servidores más críticos, las categorías de tráfico de alto riesgo y el tráfico proveniente de los segmentos de la red menos fiables (por ejemplo, priorice el descifrado de tráfico externo proveniente de socios, clientes o contratistas sobre el tráfico proveniente de un segmento interno fiable) y expanda el esfuerzo hasta aplicar el descifrado al tráfico destinado a todos sus activos del centro de datos. Descifre todo el tráfico que pueda con un rendimiento aceptable.

Excluya al tráfico inadecuado del descifrado del centro de datos. *La reglamentación y las reglas de cumplimiento para la información personal varían de un país a otro e incluso en*

las diferentes regiones de un país. Las diferentes empresas pueden tener diferentes reglas de cumplimiento para la información personal. Descifre cuanto tráfico sea posible, pero si el centro de datos aloja información que debe excluir del descifrado debido a la reglamentación o las reglas de la empresa, no descifre ese tráfico.

En Creación de reglas de aplicaciones permitidas desde el usuario al centro de datos, se crearon reglas en la política de seguridad que permiten acceso a DNS; permiten a los usuarios de ingeniería acceder a servidores de desarrollo de ingeniería, permiten a los desarrolladores de contratistas de SAP acceder únicamente a los servidores de desarrollo de SAP y permiten a un conjunto determinado de usuarios de TI acceso de gestión al servidor del centro de datos. A continuación, se crearán reglas en la política de descifrado (**Policies [Políticas]** > **Decryption [Descifrado]**) para descifrar el tráfico que permiten estas reglas.

Las reglas de la política de descifrado comparten elementos en cuanto a estos flujos de tráfico:

- Cuando crea una regla en la política de descifrado, el objetivo es descifrar tráfico, de modo que una regla en la política de seguridad pueda examinarlo y permitirlo o bloquearlo en función de la política. Para lograrlo, la regla en la política de descifrado debe usar las mismas zonas de origen y los mismos usuarios que la regla análoga en la política de seguridad, y la misma zona y dirección de destino (por lo general, las define un grupo de direcciones dinámicas, de modo que cuando añade o elimina servidores, pueda actualizar el cortafuegos sin una confirmación). Si define el mismo origen y destino en la política de seguridad y en la política de descifrado, ambas políticas se aplican al mismo tráfico.
- La Action (Acción) para todas estas reglas es decrypt (descifrar), excepto en el caso de la información personal confidencial, como se muestra en el paso 4.
- Para cada regla, configure el registro de descifrado y reenvío de logs. Registre tanto tráfico de descifrado como lo permitan los recursos de su cortafuegos.
- Las reglas de descifrado que usan inspección entrante de SSL para examinar el tráfico entrante requieren los certificados de servidor adecuados.
- Todas estas reglas de descifrado usan el mismo perfil de descifrado recomendado para el centro de datos que se muestra en Creación de perfiles de descifrado recomendados para el centro de datos.

STEP 1 | Descifre el tráfico permitido desde grupos de usuarios empleados hacia servidores del centro de datos.

Esta regla muestra cómo descifrar tráfico desde un grupo de usuarios hacia los servidores del centro de datos a los que puede acceder el grupo para brindar visibilidad del tráfico. Por ejemplo, las reglas de aplicaciones permitidas que se crearon incluyen una Regla de política de seguridad que permite a los usuarios de ingeniería acceder a los servidores de desarrollo en el centro de datos. Para proteger los servidores de desarrollo, descifre el tráfico entrante, de modo que el cortafuegos pueda inspeccionarlo y aplicar perfiles de prevención de amenazas.

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Engg to Dev Servers	User to DC BP	Engineering-Users	api-users engg-users	Engineering-DC-Infra	Dev-Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

Para crear esta regla:

- Especifique el mismo origen y destino que en la regla análoga de la política de seguridad. En este caso, los usuarios de origen son los grupos de usuarios **api-users** y **engg-users** en la zona **Engineering-Users** y el destino son los servidores que se especifican en el grupo de direcciones dinámicas **Dev-Servers** en la zona **Engineering-DC-Infra**.
- En la pestaña Options (Opciones), establezca la Action (Acción) como **Decrypt (Descifrar)** y el Type (Tipo) de descifrado como **SSL Inbound Inspection (Inspección entrante de SSL)**. Especifique el certificado de servidor para los servidores de desarrollo y aplique el perfil de descifrado recomendado

para el centro de datos a fin de aplicar los ajustes de inspección entrante de SSL y protocolo SSL al tráfico.

Cree una regla similar en la política de descifrado para el tráfico del centro de datos permitido en cada grupo de usuarios (o usuario individual, si corresponde) en función de la zona de origen y el grupo de usuarios (o usuario), y la zona de destino y el grupo de servidores (como lo define la pertenencia del grupo de direcciones dinámicas).

STEP 2 | Descifre el tráfico permitido de contratistas, socios, clientes y terceros.

Esta regla muestra cómo descifrar tráfico desde grupos externos hacia los servidores del centro de datos a los que pueden acceder. Por ejemplo, las reglas de permiso incluyen una regla en la política de seguridad que proporciona acceso limitado a contratistas de desarrollo de SAP a los servidores de la base de datos de SAP en el centro de datos. Descifre el tráfico entrante, de modo que el cortafuegos pueda inspeccionarlo, aplicar los perfiles de prevención de amenazas y proteger los servidores SAP del centro de datos.

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
SAP Contractors to SAP Servers	User to DC BP	Contractors	sap-contractors	SAP-Infra	SAP DB Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

Para crear esta regla:

- Especifique el mismo origen y destino en el tráfico a descifrar que en la regla análoga de la política de seguridad. En este caso, los usuarios de origen son el grupo de usuarios **sap-contractors** en la zona **Contractors** y el destino son los servidores que se especifican en el grupo de direcciones dinámicas **SAP DB Servers** en la zona **SAP-Infra**.
- En la pestaña Options (Opciones), establezca la Action (Acción) como **Decrypt (Descifrar)** y el Type (Tipo) de descifrado como **SSL Inbound Inspection (Inspección entrante de SSL)**. Especifique el certificado de servidor para los servidores de desarrollo y aplique el perfil de descifrado recomendado para el centro de datos a fin de aplicar los ajustes de inspección entrante de SSL y protocolo SSL al tráfico.

Cree una regla similar en la política de descifrado para el tráfico del centro de datos permitido en cada grupo de terceros en función de la zona de origen y el grupo de usuarios, y la zona de destino y el grupo de servidores (como lo define la pertenencia del grupo de direcciones dinámicas).

STEP 3 | Descifre el tráfico con acceso privilegiado a los servidores del centro de datos (a excepción del tráfico que pertenezca a información personal si la reglamentación o las reglas de cumplimiento lo prohíben).

Esta regla muestra cómo descifrar tráfico de acceso privilegiado debido a que debe descifrar cuanto tráfico sea posible para brindar la visibilidad necesaria para defender el centro de datos, independientemente de cuánto confíe en los usuarios. Si no descifra el tráfico permitido, no podrá aplicar perfiles de prevención de amenazas y si el tráfico oculta malware u otras amenazas, no las verá. En este ejemplo, se hace referencia a la regla de permiso de la política de seguridad que se ha creado previamente para brindar acceso de interfaz de gestión a los servidores del centro de datos para los superusuarios de TI.

Si el grupo de TI que gestiona y mantiene los servidores del centro de datos usa SSH, no podrá descifrar el tráfico SSH. Puede configurar el proxy SSH para bloquear túneles SSH y evitar que SSH cree un puente hacia contenido y aplicaciones potencialmente malintencionados. Si el grupo de TI usa SSL, cree una regla en la política de descifrado usando el proxy SSL de reenvío en lugar de la inspección entrante de SSL. El motivo es que la inspección entrante de SSL requiere el certificado de servidor para realizar el descifrado. Debido a que el departamento de TI gestiona varios servidores del centro de datos, crear reglas de inspección entrante de SSL para cada servidor es costoso y

resulta difícil de gestionar. El descifrado de proxy SSL de reenvío se adapta mejor en este caso de uso.

El siguiente ejemplo muestra la regla de la política de descifrado para el caso de uso de proxy SSL de reenvío.

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
IT DC Management	User to DC BP	IT-Users	it-superusers	IT-Server-Access-DC	IT-Server-Management	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

Para crear esta regla:

- Especifique el mismo origen y destino en el tráfico a descifrar que en la regla análoga de la política de seguridad. En este caso, los usuarios de Source (Origen) son el grupo de usuarios **it-superusers** en la zona **IT-Users** y Destination (Destino) son los servidores que se especifican en el grupo de direcciones dinámicas **IT-Server-Management** en la zona **IT-server-access-DC**.
- En la pestaña Options (Opciones), establezca la Action (Acción) como **Decrypt (Descifrar)** y el Type (Tipo) de descifrado como **SSL Forward Proxy (Proxy SSL de reenvío)**. Aplique el perfil de descifrado recomendado para el centro de datos para aplicar el proxy SSL de reenvío y los ajustes del protocolo SSL al tráfico.

Si otros grupos requieren acceso privilegiado, cree un tipo de regla similar en la política de descifrado para cada grupo.

El personal de TI también gestiona conmutadores, enrutadores y otros dispositivos en el centro de datos. Si el mismo grupo de usuarios de TI gestiona los mismos recursos, puede añadirlos a la zona y dirección de destino, de modo que la regla descifre tráfico de las conexiones a las interfaces de gestión de esos dispositivos. Si diferentes grupos de usuarios de TI gestionan diferentes conjuntos de recursos del centro de datos, cree reglas estrictas diferentes en la política de seguridad y las reglas correspondientes en la política de descifrado y la política de autenticación para cada grupo de usuarios.

El siguiente ejemplo muestra la regla de la política de descifrado para el caso de uso de proxy SSH. Puede decidir no descifrar el tráfico en lugar de usar el descifrado de proxy SSH.

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
IT DC Mgmt-SSH	User to DC BP	IT-Users	it-superusers	IT-Server-Access-DC	IT-Server-Management	decrypt	ssh-proxy	DC BP Decryption	none	false	true

Para crear esta regla:

- El origen y el destino del tráfico son los mismos que los del ejemplo de regla del caso de uso anterior de proxy SSL de reenvío.
- En la pestaña Options (Opciones), configure la Action (Acción) en **Decrypt (Descifrar)** y el Type (Tipo) de descifrado en **SSH Proxy (Proxy SSH)**. Aplique el perfil de descifrado recomendado para el centro de datos para aplicar los ajustes de proxy SSL y protocolo SSL al tráfico.

  El personal de TI también gestiona conmutadores, enrutadores y otros dispositivos del centro de datos. Si el mismo grupo de usuarios de TI gestiona los mismos recursos, puede añadirlos a la zona y dirección de destino, de modo que la regla descifre tráfico de las conexiones a las interfaces de gestión de esos dispositivos. Si diferentes grupos de usuarios de TI gestionan diferentes conjuntos de recursos del centro de datos, cree reglas estrictas diferentes en la política de seguridad y las reglas correspondientes en la política de descifrado y la política de autenticación para cada grupo de usuarios.

STEP 4 | No descifre información personal confidencial si la reglamentación o las reglas de cumplimiento lo prohíben.

Esta regla muestra cómo crear una exclusión de descifrado basada en la política si desea excluir tráfico del descifrado por motivos de reglamentación o de cumplimiento. En este ejemplo, se hace referencia a la regla de permiso de la política de seguridad que se creó previamente para dar acceso de servidor de finanzas para los usuarios de finanzas. Si la reglamentación o las reglas de cumplimiento le permiten descifrar este tráfico, descífrelo, de modo que el cortafuegos pueda verlo y protegerse de las amenazas.

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Finance PCI No Decrypt	User to DC BP	Finance-Users	accounting-users finance-users	Finance-DC-Infra	Fin-Servers	no-decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

Para crear esta regla:

- Especifique el mismo origen y destino en el tráfico a descifrar que en la regla análoga de la política de seguridad. En este caso, los usuarios de Source (Origen) son los grupos de usuarios **accounting-users** y **finance-users** en la zona **Finance-Users** y el Destination (Destino) son los servidores que se especifican en el grupo de direcciones dinámicas **Fin-Servers** en la zona **Finance-DC-Infra**.
- En la pestaña Options (Opciones), defina la acción como **No Decrypt (Sin descifrar)**. Aplique las prácticas recomendadas del centro de datos Sin perfil de descifrado para protegerse frente a problemas de certificados.

No aplique un perfil sin descifrado al tráfico TLSv1.3 porque la información del certificado está cifrada, por lo que el cortafuegos no puede bloquear sesiones basándose en la información del certificado.

Definición de la política de seguridad para el tráfico inicial desde internet hacia el centro de datos

Como en el resto de los flujos de tráfico en el centro de datos, controle estrictamente el tráfico que fluye desde internet hacia el centro de datos con las reglas de aplicaciones permitidas en la política de seguridad, de modo que ningún tráfico de aplicaciones desconocidas o no autorizadas pueda ingresar al centro de datos. Además, proteja los servidores web del centro de datos contra ataques de denegación de servicio (denial-of-service, DoS) aplicando reglas de la política de protección contra DoS (con perfiles de protección contra DoS) en el tráfico externo destinado al nivel del servidor web del centro de datos.

- Enfoque hacia la seguridad del tráfico desde internet hacia el centro de datos
- Creación de reglas de aplicaciones permitidas desde internet al hacia centro de datos
- Creación de reglas de la política de protección contra DoS desde internet hacia el centro de datos
- Creación de reglas para la política de descifrado desde internet hacia el centro de datos

Enfoque hacia la seguridad del tráfico desde internet hacia el centro de datos

El enfoque heredado tradicional hacia la protección del tráfico del centro de datos que fluye hacia el centro de datos desde internet expone activos valiosos al riesgo, mientras que el enfoque recomendado protege sus activos valiosos. Los principales riesgos de que el tráfico ingrese al centro de datos son descargar accidentalmente malware de un cliente externo infectado o ubicar accidentalmente malware en un servidor externo desde un servidor en riesgo en el centro de datos.

El enfoque tradicional	Riesgo	El enfoque recomendado
Cree una política de seguridad basada en los puertos.	Las aplicaciones malintencionadas acceden a la red falsificando números de puertos, creando túneles en un puerto o usando saltos de puertos para evitar la detección.	Las reglas de aplicaciones permitidas impiden que las aplicaciones se ejecuten en puertos no estándar. Registre y supervise las infracciones de la lista de permitidos. *Cuando pase de reglas basadas en el puerto a reglas basadas en la aplicación, en la base de reglas, ubique la regla basada en la aplicación sobre la regla basada en el puerto que reemplazará. Restablezca el contador de coincidencias de la regla de la política de ambas reglas. Si el tráfico coincide con la regla basada en el puerto, el conteo de coincidencias de la regla*

El enfoque tradicional	Riesgo	El enfoque recomendado
		de la política aumenta. Ajuste la regla basada en la aplicación hasta que no existan coincidencias entre el tráfico y la regla basada en el puerto durante un tiempo, y elimine la regla basada en el puerto.
Por lo general, un sistema de prevención de intrusos (Intrusion Prevention System, IPS) se implementa como un sistema de detección de intrusos (Intrusion Detection System, IDS).	Un IPS es un sistema de detección y prevención interno, mientras que un IDS es un sistema de detección externo. Implementar un IPS como un IDS excluye la detección de intrusos de la ruta de comunicación directa entre el origen y el destino, de modo que la prevención en tiempo no se produce y las amenazas pueden ingresar al centro de datos.	Dentro del cortafuegos, utilice App-ID, User-ID y Content-ID de Palo Alto Networks para crear políticas de seguridad de listas de aplicaciones permitidas que controlen el acceso de manera estricta. Aplique los perfiles de seguridad para detener amenazas conocidas y nuevas.
Un cortafuegos de aplicación web es suficiente para proteger al centro de datos.	Un atacante envía software de mando y control (C2) a un endpoint en riesgo en el centro de datos, lo que abre la red al ataque y ofrece vulnerabilidades de seguridad del lado del cliente para un ataque de abrevadero.	Evite que los atacantes envíen software de C2 a los endpoints del centro de datos asignando el perfil de seguridad antispyware estricto a la regla de la política de seguridad que controla el tráfico. Este perfil es una de las funciones incluidas en el cortafuegos, de modo que no debe realizar inversiones adicionales para aplicar esta protección.

Creación de reglas de aplicaciones permitidas desde internet al hacia centro de datos

Los principales riesgos de que el tráfico acceda al centro de datos desde internet son descargar accidentalmente malware de un cliente externo infectado o ubicar accidentalmente malware en un servidor externo si un cliente retira datos de un servidor en riesgo en su centro de datos. Proteja el tráfico desde internet hacia el centro de datos, de modo que no descargue accidentalmente malware que aprovecha las vulnerabilidades del servidor o permita que un cliente descargue malware de uno de los servidores de su empresa que pueda infectar a los socios y a los clientes, o termine en un sitio web que usa su sector (y permita un ataque de abrevadero).

Asegúrese de que el origen del tráfico hacia el centro de datos no provenga de direcciones IP malintencionadas u otros orígenes potencialmente riesgosos, y que solo permita aplicaciones necesarias por motivos empresariales. No permita aplicaciones innecesarias (y, en especial, desconocidas) en el centro de datos. Para hacerlo:

- Cree reglas de permitidos que controlen las aplicaciones autorizadas y permitidas que los dispositivos externos pueden usar para comunicarse con el centro de datos.

Etiquete todas las aplicaciones sancionadas *con la etiqueta Sanctioned (Sancionado) predefinida. Panorama y los cortafuegos consideran a las aplicaciones sin la etiqueta Sanctioned (Sancionado) como aplicaciones no sancionadas.*

- Cree una lista dinámica externa para identificar direcciones IP defectuosas y usarla para evitar que accedan a su centro de datos.
- Cree una aplicación personalizada para las aplicaciones exclusivas, de modo que pueda identificar la aplicación y aplicar seguridad a ella.

  Si posee políticas existentes de cancelación de aplicaciones que creó únicamente para definir los tiempos de espera personalizados de una sesión en un conjunto de puertos, convierta las políticas existentes de cancelación de aplicaciones en políticas basadas en la aplicación configurando los tiempos de espera de una sesión basados en el servicio para conservar el tiempo de espera personalizado de cada aplicación y migrar la regla a una regla basada en la aplicación. Las políticas de cancelación de aplicaciones se basan en los puertos. Cuando usa políticas de cancelación de aplicaciones para conservar los tiempos de espera personalizados de una sesión en un conjunto de puertos, pierde visibilidad de la aplicación respecto a esos flujos, de modo que no sabe ni controla las aplicaciones que usan los puertos. Los tiempos de espera de una sesión basados en el servicio logran tiempos de espera personalizados y conservan la visibilidad de la aplicación.
- Aplique el grupo de perfiles de seguridad de prácticas recomendadas, que consta de los perfiles de seguridad de prácticas recomendadas para permitir que las reglas protejan frente a malware, vulnerabilidades, tráfico C2 y amenazas conocidas y desconocidas.
- Registre todo el tráfico permitido al final de la sesión para realizar un seguimiento y analizar las infracciones de reglas. Reenvíe los logs a los servidores de logs y, cuando corresponda, reenvíe los correos electrónicos de logs a los administradores correspondientes.

Orden de la base de reglas de la política de seguridad del centro de datos le muestra cómo ordenar estas reglas con todas las otras reglas que creamos para los otros tres flujos de tráfico en el centro de datos y las reglas de bloqueo, de modo que ninguna regla enmascareque a otra.

Para aplicar una política de seguridad uniforme en varios centros de datos, puede reusar las plantillas y las pilas de plantillas, de modo que las mismas políticas se apliquen en cada centro de datos. Las plantillas usan variables para aplicar valores para dispositivos específicos como direcciones IP, FQDN, etc., conservar una política de seguridad global y reducir el número de plantillas y pilas de plantillas que debe gestionar.

Permita tráfico de aplicaciones sancionadas de proveedores, contratistas y clientes, que se restringe solo a las aplicaciones necesarias.

Esta regla muestra cómo proteger el tráfico de aplicaciones que llega al centro de datos proveniente de orígenes externos controlando estrictamente las aplicaciones permitidas, lo que solo las permite en el puerto predeterminado y bloquea los orígenes que conoce como defectuosos usando una lista dinámica externa para identificar direcciones IP defectuosas conocidas.

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Web Server Inbound	Internet to DC...	universal	L3-External	~~Bad IPs List~~	any	any	Web-Server-Tier-DC	Web Servers	any	Acme	application-default	Allow		

Para crear esta regla:

- Evite que los orígenes defectuosos conocidos intenten acceder al centro de datos. Use la opción **Negate (Negar)** en la **Source Address (Dirección de origen)** de la regla de la política de seguridad para bloquear conexiones de direcciones IP malintencionadas. En este ejemplo, se usa una lista dinámica externa (**Bad IPs List [Lista de IP malintencionadas]**) para identificar las direcciones IP

malintencionadas conocidas y bloquearlas. (El texto tachado en la dirección de origen indica que se niega en lugar de permitirse).
- Limite las aplicaciones a únicamente las aplicaciones necesarias por motivos empresariales y permita que se ejecuten únicamente en sus puertos predeterminados (**application-default**) para evitar que el malware evasivo intente ejecutarse en puertos no estándar. En este ejemplo, el proveedor usa una aplicación exclusiva denominada **Acme**. Se creó una aplicación personalizada para identificar la aplicación exclusiva **Acme**, de modo que el cortafuegos pueda clasificar el tráfico y aplicar la política de seguridad adecuada.
- Limite el destino del tráfico de la aplicación **Acme** al grupo de direcciones dinámicas **Web-Servers** en la zona **Web-Server-Tier-DC**. Si la dirección de destino no se encuentra en el nivel del servidor web, el cortafuegos bloquea el tráfico.

Verifique que solo se ejecuten las aplicaciones que permitió explícitamente en las reglas de la política de seguridad viendo el informe de aplicaciones predefinido [**Monitor (Supervisar)** > **Reports (Informes)** > **Application Reports (Informes de aplicación)** > **Applications (Aplicaciones)**]. Si ve aplicaciones inesperadas en el informe, revise las reglas de aplicaciones permitidas y vuelva a ajustarlas, de modo que no permitan aplicaciones inesperadas.

Creación de reglas para la política de descifrado desde internet hacia el centro de datos

Cree reglas de la política de descifrado para proporcionar visibilidad del tráfico que accede al centro de datos procedente de internet, de modo que pueda aplicar la política de seguridad a ese tráfico. Cuando cree una regla en la política de seguridad que permite el acceso a un conjunto de servidores de centro de datos, cree una regla en la política de descifrado para descifrar el tráfico. En Creación de reglas de aplicaciones permitidas desde internet al hacia centro de datos, creamos una regla de política de seguridad que permite el acceso desde Internet al nivel del servidor web en el centro de datos, utilizando solo aplicaciones permitidas. A continuación, creamos una regla en la política de descifrado [**Policies (Políticas)** > **Decryption (Descifrado)**] para descifrar el tráfico que permite esta regla.

Para descifrar el tráfico de modo que una regla en la política de seguridad pueda examinarlo y permitir o bloquearlo en función de la política, la regla en la política de descifrado debe usar las mismas zonas de origen y los mismos usuarios que la regla análoga en la política de seguridad, y la misma zona y dirección de destino (por lo general, las define un grupo de direcciones dinámicas, de modo que cuando añade o elimina servidores, pueda actualizar el cortafuegos sin una confirmación). Si define el mismo origen y destino en la política de seguridad y en la política de descifrado, ambas políticas se aplican al mismo tráfico.

La regla de descifrado usa el mismo perfil de descifrado recomendado para el centro de datos que se muestra en Creación de perfiles de descifrado recomendados para el centro de datos.

Para cada regla, configure el registro de descifrado y reenvío de logs. Registre tanto tráfico de descifrado como lo permitan los recursos de su cortafuegos.

STEP 1 | Descifre el tráfico permitido desde internet hacia los servidores web del centro de datos.

Esta regla muestra cómo descifrar el tráfico de conexiones iniciadas de manera externa hacia el centro de datos. Por ejemplo, las reglas de aplicaciones permitidas que creamos habilitan el acceso de tráfico externo a los servidores web del centro de datos usando únicamente determinadas aplicaciones. Para proteger los servidores web del centro de datos, descifre el tráfico, de modo que el cortafuegos pueda inspeccionarlo y aplicar perfiles de prevención de amenazas.

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Internet to DC	Internet to DC BP	L3-External	any	Web-Server-Tier-DC	Web Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

Para crear esta regla:

- Especifique el mismo origen y destino que en la regla análoga de la política de seguridad. En este caso, el origen es la zona **L3-External** y el destino son los servidores que se especifican en el grupo de direcciones dinámicas **Web-Servers** en la zona **Web-Server-Tier-DC**.
- En la pestaña Options (Opciones), establezca la Action (Acción) como **Decrypt (Descifrar)** y el Type (Tipo) de descifrado como **SSL Inbound Inspection (Inspección entrante de SSL)**. Especifique el certificado de servidor para los servidores web y aplique el perfil de descifrado recomendado para el centro de datos a fin de aplicar los ajustes de inspección entrante de SSL y protocolo SSL al tráfico.

STEP 2 | Cree reglas de la política de descifrado similares para el tráfico proveniente de internet hacia cualquier otro grupo de servidores si se permite el acceso y para las otras aplicaciones que permite.

Creación de reglas de la política de protección contra DoS desde internet hacia el centro de datos

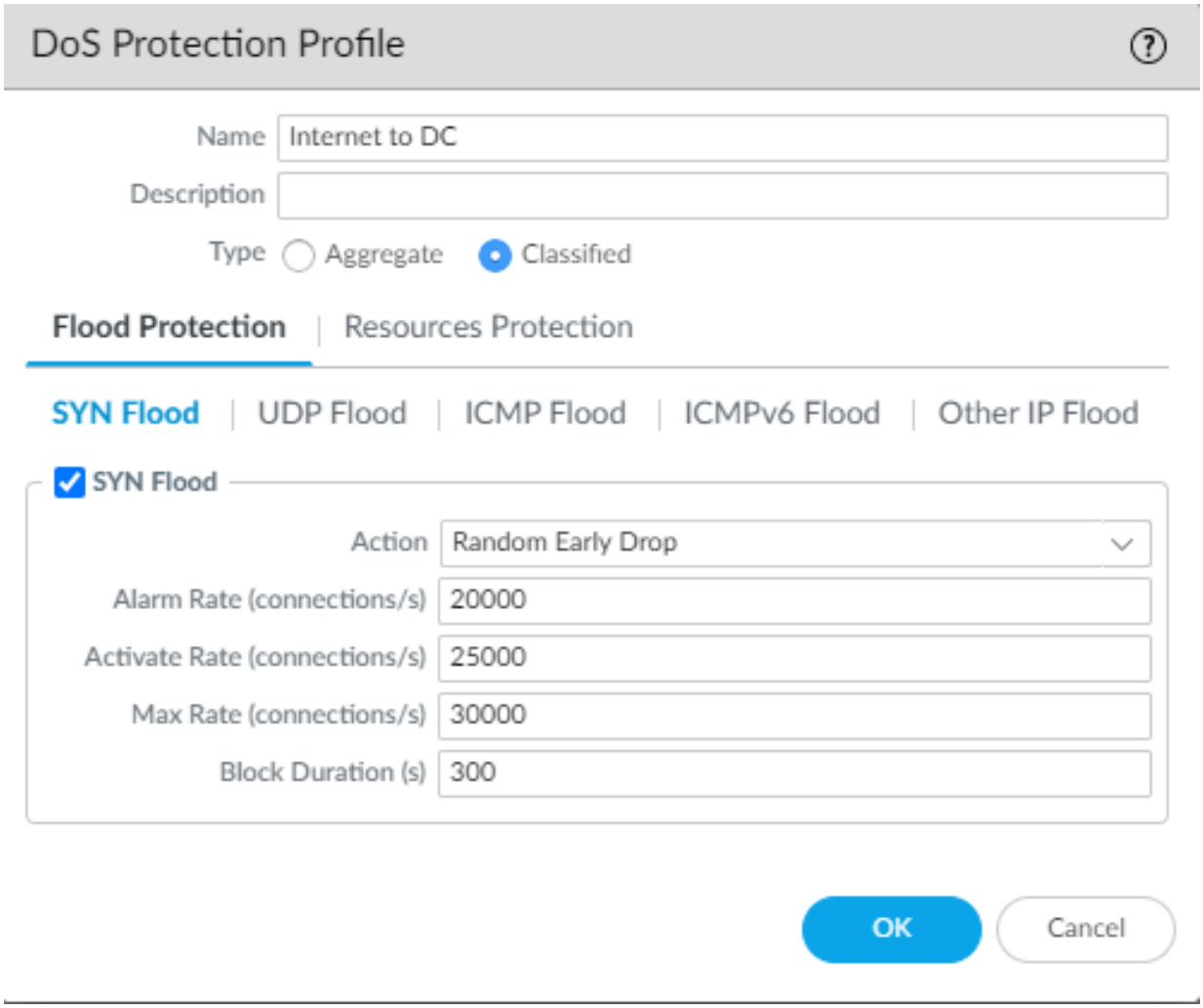
Un método que usan los atacantes para perjudicar a una red es un ataque de denegación de servicio (Denial-of-Service, DoS) que intenta superar los sistemas objetivo conectados a internet, eliminarlos y evitar que estén disponibles para todos los usuarios y servicios legítimos. Los servidores web del centro de datos son un objetivo atractivo debido a que si no funcionan, se pierde gran parte del acceso legítimo al centro de datos.

Proteja el nivel del servidor web del centro de datos aplicando una política de protección contra DoS clasificada al tráfico de internet destinado a estos servidores. Una política de protección contra DoS clasificada aplica un perfil de protección contra DoS clasificado que controla el número de conexiones entrantes al tráfico que se define en la política.

Además, configure la protección de búfer de paquetes de cada zona para proteger al cortafuegos contra ataques de DoS de una sesión que puedan sobrecargar el búfer de paquetes del cortafuegos y causar que se bloquee tráfico legítimo, en especial, en cortafuegos que protegen servicios críticos.

STEP 1 | Cree un perfil de protección contra DoS clasificado que proteja a los servidores web del centro de datos de ataques de DoS limitando el número de conexiones por segundo para evitar un ataque de inundación SYN.

Este perfil de protección contra DoS limita el número de conexiones por segundo (connections-per-second, CPS) del tráfico que se define en las reglas de la política de protección contra DoS a la que adjunta el perfil para evitar que un ataque de DoS inhabilite sus servidores web. El perfil establece umbrales de CPS progresivos para alertarle, para activar el descarte de paquetes de descarte aleatorio temprano (Random Early Drop, RED) y para bloquear las conexiones nuevas, además de un período durante el que las conexiones nuevas permanecen bloqueadas. Los umbrales de CPS que configura para proteger los servidores web del centro de datos dependen de la capacidad de sus servidores web.



Para crear este perfil:

- En **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **DoS Protection (Protección contra DoS)**, haga clic en **Add (Añadir)** para añadir un perfil de protección contra DoS clasificado.
- Asigne un **Name (Nombre)** al perfil, seleccione **Classified (Clasificado)** como **Type (Tipo)** de perfil, configure los valores de CPS para que envíen una alerta [**Alarm Rate (Tasa de alarma)**], activen el RED [**Activate Rate (Tasa de activación)**], comiencen a bloquear sesiones nuevas [**Max Rate (Tasa máx.)**], y configure el periodo de tiempo en segundos antes de bloquear sesiones nuevas [**Block Duration (Duración de bloqueo)**] cuando la tasa de CPS alcanza el umbral de **Max Rate (Tasa máx.)**.

Si no usa protocolos como UDP u otros protocolos de IP, limítelos usando una combinación de reglas de política de seguridad para permitir aplicaciones y perfiles de protección de zonas *para bloquear protocolos que no se usan con el ajuste de las CPS de protección contra inundaciones en cero paquetes en los protocolos que desea bloquear.*

STEP 2 | Cree una regla clasificada en la política de protección contra DoS para definir los servidores que desea proteger contra ataques de DoS y adjunte el perfil de protección contra DoS.

Esta regla evita que un ataque de inundación SYN inhabilite el nivel de servidor web de su centro de datos. En este ejemplo, se aplica el perfil de protección contra DoS clasificado al tráfico externo que puede conectarse al nivel de servidor web.

		Source			Destination				Protection		
NAME	TAGS	ZONE/INTERFACE	ADDRESS	USER	ZONE/INTERFACE	ADDRESS	SERVICE	ACTION	AGGREGATE	CLASSIFIED	LOG FORWARDING
DC Web Server Protection	Internet to DC BP	L3-External	~~Bad IPs List~~	any	Web-Server-Tier-DC	Web Servers	service-http service-https	protect	none	profile: Internet to DC destination-ip-only	DoS-LF

Para crear esta regla:

- Para aplicar la protección contra DoS al tráfico que se dirige al nivel de servidor web, la política de protección contra DoS debe aplicarse al mismo tráfico que se aplica la regla de la política de seguridad que permite el tráfico. En este ejemplo, esta regla DoS protege el tráfico que permitimos en Creación de reglas de aplicaciones permitidas desde internet al hacia centro de datos.
- En la pestaña Option/Protection (Opción/Protección), especifique los servicios web (**service-http** y **service-https**), configure la Action (Acción) en **protect (proteger)** para aplicar los umbrales de inundación SYN del perfil de protección contra DoS al tráfico, configure el método de reenvío de logs (si ya configuró el reenvío de logs) y seleccione el perfil de protección contra DoS clasificado que se configuró para el tráfico en el paso anterior (**Internet to DC**).

Para protegerse de ataques internos de inundaciones SYN, cree una regla separada en la política de protección contra DoS que especifique las zonas internas como la zona de origen en lugar de **L3-External**. Crear reglas separadas para orígenes de ataques externos e internos permite generar informes separados que agilizan la investigación de los intentos de ataque.

Definición de la política de seguridad para el tráfico inicial desde el centro de datos hacia internet

Según la arquitectura del centro de datos, los servidores en el centro de datos pueden conectarse a internet para obtener actualizaciones de software o para comprobar el estado de revocación de certificados del servidor. El centro de datos es el lugar ideal para los adversarios que se ocultan debido a que los planes de seguridad se centran en la comunicación con el usuario y omiten los servidores que se comunican con internet. Cuando los servidores del centro de datos inician una comunicación directa con internet, debe protegerse contra varios riesgos de seguridad:

- **Filtración de datos:** los atacantes usan aplicaciones legítimas como FTP o HTTP, u otros métodos como tunelización de DNS para robar datos. Cree una lista de permitidos de la regla de política de seguridad de la aplicación que permita solo las aplicaciones necesarias para las actualizaciones del servidor, de modo que el resto de las aplicaciones se bloqueen, incluso si son aplicaciones legítimas en otras circunstancias. Las reglas flexibles de aplicaciones ofrecen oportunidades a los atacantes.
- **Mando y control (Command-and-control, C2) que usa aplicaciones legítimas:** si los servidores del centro de datos pueden comunicarse con internet usando aplicaciones legítimas que no se usan para las actualizaciones de software, es posible que los atacantes usen esas aplicaciones legítimas para actividades de C2. Por ejemplo, permitir la navegación web en puertos no estándar crea oportunidades para los atacantes. Los servidores solo deben poder comunicarse con internet usando únicamente las aplicaciones específicas necesarias para las actualizaciones de software en los puertos predeterminados y no otras aplicaciones, incluso si esas aplicaciones son legítimas y sancionadas para otros usos.
- **Descargar malware adicional:** si un atacante pone el servidor del centro de datos en riesgo, es posible que el malware en el servidor descargue más malware de internet enviando información a su origen o con otro mecanismo. Una regla de permiso estricta que solo permita la comunicación con los servidores de actualización adecuados con únicamente las aplicaciones de actualización necesarias evita que los atacantes se comuniquen con sitios web que alojan malware y que se filtren datos. Además, instale Cortex XDR Agent en los servidores (y en todos los endpoints) del centro de datos para evitar que el malware que ya reside en un servidor se ejecute.

Enfoques hacia la seguridad del tráfico desde el centro de datos hacia internet

El enfoque heredado tradicional de proteger el tráfico del centro de datos que fluye hacia internet expone activos valiosos al riesgo, mientras que el enfoque recomendado protege sus activos valiosos.

El enfoque tradicional	Riesgo	El enfoque recomendado
Cree reglas basadas en el puerto o reglas basadas en IP, que brindan suficiente	Las reglas basadas en puertos y basadas en IP no pueden controlar qué aplicaciones pueden conectarse a internet. Si un puerto está activo,	Cree reglas de permiso estrictas basadas en aplicaciones que permitan que los servidores en el centro de datos que recuperan actualizaciones solo usen aplicaciones legítimas para comunicarse solo con otros servidores de

El enfoque tradicional	Riesgo	El enfoque recomendado
seguridad en la red fiable.	cualquier aplicación puede usarlo.	actualización legítimos. Registre y supervise las infracciones de la reglas de permiso.  *Cuando pase de reglas basadas en el puerto a reglas basadas en la aplicación, en la base de reglas, ubique la regla basada en la aplicación sobre la regla basada en el puerto que reemplazará. Restablezca el contador de coincidencias de la regla de la política de ambas reglas. Si el tráfico coincide con la regla basada en el puerto, el conteo de coincidencias de la regla de la política aumenta. Ajuste la regla basada en la aplicación hasta que no existan coincidencias entre el tráfico y la regla basada en el puerto durante un tiempo, y elimine la regla basada en el puerto.*
Los servidores del centro de datos solo se comunican con servidores fiables como servidores de actualización, de modo que el descifrado de ese tráfico es innecesario.	Es posible que el malware o el software de mando y control que ya se encuentra en el centro de datos intente comunicarse con servidores externos para descargar más malware o filtrar datos.	Descifre todo el tráfico desde el centro de datos hacia internet. Cree una categoría de URL personalizada que defina que los servidores en el centro de datos de las URL pueden comunicarse y usarlas en la política de seguridad para limitar el acceso a internet con servidores externos. Use la misma URL personalizada en la política de descifrado para descifrar el tráfico hacia los servidores externos.
Combine el bloqueo y las alertas de los perfiles de prevención de amenazas de varios proveedores.	Un conjunto de herramientas individuales ofrece brechas de seguridad a los atacantes y es posible que no funcionen adecuadamente.	El conjunto de herramientas de seguridad coordinada de Palo Alto Networks trabaja en conjunto para encender la seguridad y evitar ataques.

Creación de reglas para aplicaciones permitidas desde el centro de datos hacia internet

El principal caso de uso de servidores de centros de datos que inician conexiones con servidores externos en internet es para actualizar software u obtener el estado del certificado. El principal riesgo es conectarse al servidor incorrecto, en especial, en el caso de las actualizaciones de Linux debido a que existen demasiadas URL externas a las que podrían conectarse accidentalmente. Asegúrese de que los servidores de centros de datos reciban actualizaciones de servidores de actualización legítimos, que usen únicamente las aplicaciones necesarias en los puertos predeterminados.

Para hacerlo, cree reglas estrictas de aplicaciones permitidas que limiten los servidores externos a los que se conectan los servidores de centros de datos y las aplicaciones que usan los servidores de los centros de datos cuando se conectan a servidores externos. Etiquete todas las aplicaciones sancionadas con la etiqueta *Sanctioned (Sancionado)* predefinida. (Panorama y los cortafuegos consideran a las aplicaciones sin la etiqueta Sanctioned [Sancionado] como aplicaciones no sancionadas). Un conjunto de reglas de aplicaciones permitidas estricto interrumpe posibles ataques al:

- Evitar que el malware que ya se encuentra en un servidor del centro de datos se conecte a un servidor externo en riesgo (*envíe información a su origen*) y descargue datos adicionales debido a que las reglas de permiso no permiten las conexiones a esos servidores.
- Evitar que los atacantes usen aplicaciones legítimas como FTP, HTTP o la tunelización de DNS para filtrar datos, o que usen aplicaciones legítimas como la navegación web o puertos no estándar para operaciones de mando y control (command-and-control, C2) debido a que las reglas de permiso no permiten que los servidores del centro de datos se comuniquen con internet usando esas aplicaciones. Otra manera de evitar la filtración es usar el control de **Direction (Dirección)** del perfil de bloqueo de archivos para bloquear archivos de actualización salientes, de modo que solo permita la descarga de archivos de actualización de software.

Cree una regla de permitidos estricta para cada aplicación que requiera actualizaciones de software de un conjunto diferente de servidores externos. En muchos casos, App-ID no es suficiente para proteger los servidores del centro de datos. Por ejemplo, en el caso de las actualizaciones en servidores Linux, no es suficiente limitar el tráfico a una aplicación de actualización como *yum* o *apt-get* debido a que no evita que se conecten a servidores ilegítimos. Se recomienda buscar las direcciones URL a las que los servidores del centro de datos deben conectarse, crear categorías de URL personalizadas (**Objects [Objetos]** > **Custom Objects [Objetos personalizados]** > **URL Category [Categoría de URL]**) que especifiquen los sitios web a usar y combinarlas con App-ID en las reglas de la política de seguridad. La combinación de App-ID y las categorías personalizadas de URL bloquea a los servidores externos con los que se pueden conectar los servidores del centro de datos evitando que usen aplicaciones ilegítimas y evitando conexiones a servidores de actualización que no se encuentren en la categoría personalizada de URL. Por ejemplo, en un regla de la política de seguridad que permite que los servidores del centro de datos se conecten a servidores de actualización de CentOS, puede crear una categoría personalizada de URL denominada *CentOS-Update-Servers* y añadir los sitios de actualización de CentOS que usan sus servidores a la categoría personalizada.

Para descubrir las URL de servidores de actualización de Linux legítimos y otros servidores de actualización, trabaje con el equipo de ingeniería de software, de operaciones de desarrollo y otros grupos que realicen actualizaciones de software para comprender adónde se dirigen cuando desean obtener actualizaciones. También puede registrar sesiones de navegación web, recopilar las URL a las que se conectan los desarrolladores y dirigir las URL a ingeniería para filtrar las URL correctas de la política de seguridad.

No use el perfil de filtrado de URL (filtrado de URL PAN-DB) en las reglas de la política de seguridad para los servidores del centro de datos que se comunican con internet debido

a que no desea permitir todos los servidores de actualización. Restrinja la comunicación, de modo que los servidores del centro de datos solo puedan comunicarse con servidores específicos donde obtienen actualizaciones.

Además, toda la comunicación permitida debe producirse en los puertos estándar de cada aplicación. Las aplicaciones no deben ejecutarse en puertos no estándar. Como con todo el tráfico del centro de datos, supervise los incumplimientos de la regla de permitidos ya que estos indican si debe actualizar la política de seguridad para permitir tráfico legítimo o si un adversario intenta acceder o accedió a la red.

Orden de la base de reglas de la política de seguridad del centro de datos le muestra cómo ordenar estas reglas con todas las otras reglas que creamos para los otros tres flujos de tráfico en el centro de datos y las reglas de bloqueo, de modo que ninguna regla enmascareque a otra.

Para aplicar una política de seguridad uniforme en varios centros de datos, puede reusar las plantillas y las pilas de plantillas, de modo que las mismas políticas se apliquen en cada centro de datos. Las plantillas usan variables para aplicar valores para dispositivos específicos como direcciones IP, FQDN, etc., conservar una política de seguridad global y reducir el número de plantillas y pilas de plantillas que debe gestionar.

Cada una de las siguientes reglas de permiso:

- Tiene la práctica recomendada grupo de perfiles de seguridad adjunta, que consta de los perfiles de seguridad de práctica recomendada. El uso de un grupo de perfiles de seguridad le permite aplicar todos los perfiles de prácticas recomendadas a una regla a la vez en lugar de especificar cada perfil individualmente. Los grupos de perfiles de seguridad hacen que la configuración de la protección contra malware, vulnerabilidades, tráfico C2 y amenazas conocidas y desconocidas sea más rápida y sencilla.
- Registra el tráfico (al final de la sesión) para que pueda realizar un seguimiento y analizar las infracciones de las reglas, e incluye el reenvío de logs. Reenvíe los logs a los servidores de logs y, cuando corresponda, reenvíe los correos electrónicos de logs a los administradores correspondientes.

STEP 1 | Permita que los servidores del centro de datos accedan a los servidores de actualización de software.

Esta regla muestra cómo limitar el acceso a los servidores de actualización de software en internet, de modo que los servidores del centro de datos se comuniquen únicamente con servidores legítimos conocidos y no se comuniquen con otros servidores de actualización externos. En este ejemplo, se permite que los servidores del centro de datos de ingeniería accedan a los servidores de actualización de CentOS y se limita la comunicación al uso de solo las aplicaciones necesarias para establecer conexiones con los conjuntos adecuados de servidores de actualización.

			Source			Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
CentOS Update	DC to Internet BP	universal	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	yum	application-default	CentOS-Update-Servers	Allow		

Para crear esta regla:

- Limite el origen de las solicitudes de actualización de CentOS a solo los servidores del centro de datos que deben recuperar actualizaciones, en este ejemplo, el grupo de direcciones dinámicas **Dev-Servers** en la zona **Engineering-DC-Infra**.
- Limite las aplicaciones que pueden usar los servidores del centro de datos para comunicarse con servidores de actualización externos únicamente a las aplicaciones necesarias, en este ejemplo, **yum** para las actualizaciones de CentOS. Permita que las aplicaciones únicamente se ejecuten en puertos predeterminados para evitar que el malware evasivo intente usar puertos no estándar.
- Cree una categoría personalizada de URL para definir las URL de los servidores de actualización a los que se pueden conectar los servidores del centro de datos. En este ejemplo, la categoría

personalizada de URL **CentOS-Update-Servers** define las URL del servidor de actualización con las que se pueden comunicar los servidores del centro de datos.

Esta combinación de limitación también evita que los atacantes que ya pusieron el servidores del centro de datos en riesgo se comuniquen con otros destinos y usen otras aplicaciones para filtrar datos o descargar malware adicional.

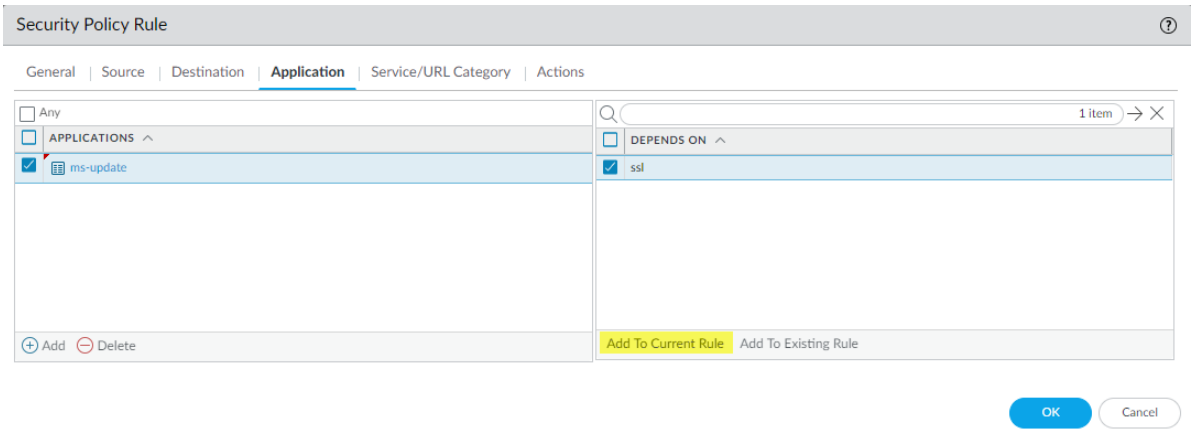
De manera similar, una regla que permita a los mismos servidores comunicarse con los servidores de actualización de Microsoft Windows usa la misma construcción.

			Source			Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
Windows Update	DC to Internet BP	universal	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	ms-update ssl	application-default	Win-Update-Servers	Allow		

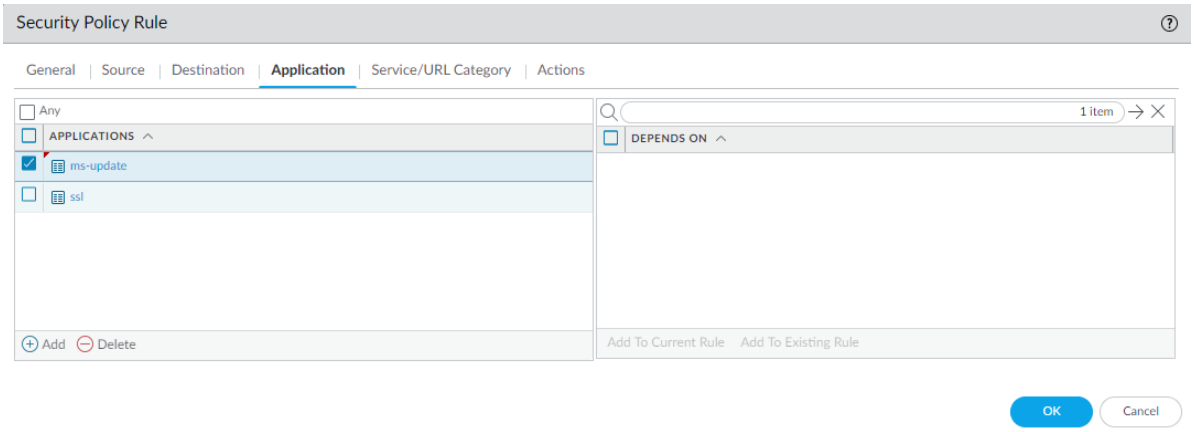
La zona de origen y la dirección son las mismas que en la regla de actualización de CentOS anterior. Las diferencias son las siguientes:

- La categoría personalizada de URL (**Win-Update-Servers**) contiene la URL de las actualizaciones de Windows, de modo que el contacto con otras URL se bloquea.
- Las aplicaciones pertenecen a las actualizaciones de Windows. Además de la aplicación **ms-update**, las actualizaciones de Microsoft requieren la aplicación **ssl** debido a que ms-update depende de SSL. Como en la regla de actualización de CentOS, solo los puertos estándar son válidos.

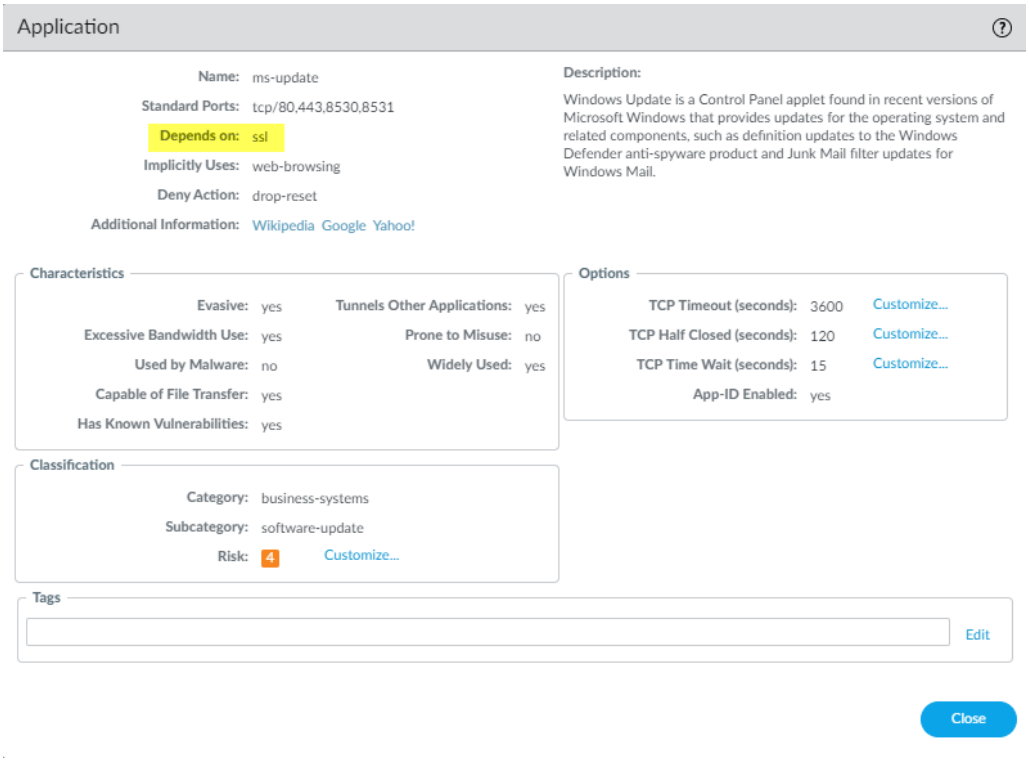
  Algunas aplicaciones dependen de otras aplicaciones. Para una aplicación determinada, debe permitir todas las aplicaciones dependientes o la aplicación no funcionará. La interfaz de usuario muestra las dependencias de la aplicación cuando crea una regla de política de seguridad. Por ejemplo, cuando especifica la aplicación ms-update en la regla, la interfaz muestra que ms-update también depende del permiso SSL:



  Haga clic en **Add to Current Rule (Añadir a la regla actual)** para añadir las aplicaciones seleccionadas a la regla.



También puede utilizar la función de búsqueda [Objects (Objetos) > Applications (Aplicaciones)] para encontrar dependencias de aplicaciones. Por ejemplo, para encontrar las dependencias para la aplicación ms-update, busque ms-update, haga clic en la aplicación ms-update en la lista de aplicaciones resultante y luego marque el campo Depend on: (Depende de:).



STEP 2 | Permita que los servidores del centro de datos accedan a los servidores de actualización de DNS y NTP.

Esta regla muestra cómo limitar el acceso a los servidores de actualización de DNS y NTP en internet, de modo que los servidores del centro de datos se comuniquen únicamente con servidores legítimos conocidos. En este ejemplo, se permite que los servidores del centro de datos de TI accedan a los servidores de actualización de DNS y NTP, y se limita la comunicación al uso de solo las aplicaciones necesarias para establecer conexiones con los conjuntos adecuados de servidores de actualización.

NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	ZONE	ADDRESS						
NTP DNS Update	DC to Internet BP	universal	IT Infrastructure	DNS-NTP-Servers	any	L3-External	any	dns ntp	application-default	NTP-DNS-Update-Servers	Allow		

Para crear esta regla:

- Limite el origen de las solicitudes de actualización de DNS y NTP a solo los servidores del centro de datos que deben recuperar actualizaciones, en este ejemplo, el grupo de direcciones dinámicas **DNS-NTP-Servers** en la zona **Engineering-DC-Infra**.
- Limite las aplicaciones que pueden usar los servidores del centro de datos para comunicarse con servidores de actualización externos únicamente a las aplicaciones necesarias, en este ejemplo, **dns** y **ntp**. Permita que las aplicaciones únicamente se ejecuten en puertos predeterminados para evitar que el malware evasivo intente usar puertos no estándar.
- Cree una categoría personalizada de URL para definir las URL de los servidores de actualización a los que se pueden conectar los servidores del centro de datos. En este ejemplo, la categoría personalizada de URL **NTP-DNS-Update-Servers** define las URL del servidor de actualización con las que se pueden comunicar los servidores del centro de datos.

STEP 3 | Permita que los servidores del centro de datos accedan a los servidores de entidades de certificación para obtener el estado de revocación de los certificados digitales y asegúrese de que sean válidos.

Esta regla permite a los servidores del centro de datos conectarse a un respondedor (servidor) de protocolo de estado de certificado en línea (Online Certificate Status Protocol, OCSP) en internet para comprobar el estado de revocación de los certificados de autenticación. Un respondedor de OCSP brinda el estado más reciente del certificado en comparación con las actualizaciones de la lista de revocación de certificados (Certificate Revocation List, CRL) del navegación, que dependen de la frecuencia con la que se actualice el navegador de la CRL para estar al día con las revocaciones de certificados, de modo que es más probable que la CRL esté desactualizada que un respondedor de OCSP. Cuando configura un perfil de certificado en el cortafuegos, puede configurar la verificación de estado de CRL como método de reserva para el OCSP en caso de que el respondedor del OCSP no se pueda comunicar.

NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	ZONE	ADDRESS					
Cert Update	DC to Internet BP	universal	IT Infrastructure	IT-Server-Management	any	L3-External	any	ocsp	application-default	Allow		

Para crear esta regla:

- Limite el origen de las solicitudes de comprobación de la revocación de certificados a solo los servidores del centro de datos que deben comprobar la validación de certificados, en este ejemplo, el grupo de direcciones dinámicas **IT-Server-Management** en la zona **IT-Infrastructure**.
- Limite las aplicaciones que pueden usar los servidores del centro de datos para comunicarse con servidores de revocación de certificados externos únicamente a las aplicaciones necesarias. En este ejemplo, se protege la conexión entre los servidores del centro de datos y los respondedores de OCSP, de modo que la única aplicación que se debe especificar es **ocsp**. Permita que las aplicaciones únicamente se ejecuten en puertos predeterminados para evitar que el malware evasivo intente usar puertos no estándar.

Verifique que solo se ejecuten las aplicaciones que tienen permiso explícito en las reglas de la política de seguridad viendo el informe de aplicaciones predefinido (**Monitor [Supervisar]** > **Reports [Informes]** > **Application Reports [Informes de aplicación]** > **Applications [Aplicaciones]**). Si ve aplicaciones inesperadas en el informe, revise las reglas de aplicaciones permitidas y vuelva a ajustarlas, de modo que no permitan aplicaciones inesperadas.

Creación de reglas para la política de descifrado desde el centro de datos hacia internet

Cree reglas en la política de descifrado para brindar visibilidad del tráfico desde los servidores del centro de datos hacia internet. Descifre todo el tráfico desde los servidores del centro de datos hacia internet. Las únicas cuentas que inician conexiones a internet desde el interior del centro de datos son las cuentas de servicio y la mayoría del tráfico pertenece a actualizaciones de software, de modo que no existen problemas de privacidad que deban considerarse. Es importante descifrar e inspeccionar este tráfico debido a que si un servidor de actualización se encuentra en riesgo, los servidores del centro de datos pueden descargar malware y propagarlo con el proceso de actualización de software. Inspeccionar el tráfico y aplicar perfiles recomendados de prevención de amenazas protege al centro de datos de malware que, de lo contrario, se descargaría de un servidor de actualización legítimo usando una aplicación legítima.

En Creación de reglas para aplicaciones permitidas desde el centro de datos hacia internet, se crearon reglas de la política de seguridad que permiten a los servidores del centro de datos inician conexiones con servidores de actualización en internet para actualizar el software del sistema operativo, DNS, NTP y para comprobar certificados. A continuación, se crearan reglas análogas de la política de descifrado para descifrar el tráfico que permiten las reglas de la política de seguridad de actualización.

No descifre el tráfico dirigido a servidores de revocación de certificados (respondedor en línea). Por lo general, el tráfico del protocolo de estado de certificado en línea (Online Certificate Status Protocol, OCSP) usa HTTP, de modo que el tráfico es texto no cifrado. Además, es posible que el descifrado de proxy SSL de reenvío interrumpa el proceso de actualización debido a que el cortafuegos actúa como un proxy de man-in-the-middle (intermediario) y reemplaza el certificado de cliente con un certificado proxy, que es posible que el respondedor de OCSP no acepte como válido.

Las reglas de la política de descifrado comparten elementos en cuanto a estos flujos de tráfico:

- Cuando crea una regla en la política de descifrado, el objetivo es descifrar tráfico, de modo que una regla en la política de seguridad pueda examinarlo y permitirlo o bloquearlo en función de la política. Para lograrlo, la regla en la política de descifrado debe usar las mismas zonas de origen y los mismos usuarios que la regla análoga en la política de seguridad, y la misma zona y dirección de destino (por lo general, las define un grupo de direcciones dinámicas, de modo que cuando añade o elimina servidores, pueda actualizar el cortafuegos sin una confirmación). Si define el mismo origen y destino en la política de seguridad y en la política de descifrado, ambas políticas se aplican al mismo tráfico.
- La acción para todas estas reglas es descifrar.
- Para cada regla, configure el registro de descifrado y reenvío de logs. Registre tanto tráfico de descifrado como lo permitan los recursos de su cortafuegos.
- Todas estas reglas de descifrado usan el mismo perfil de descifrado recomendado para el centro de datos que se muestra en Creación de perfiles de descifrado recomendados para el centro de datos.

En muchos casos, los ejemplos de reglas de la política de descifrado incluyen una categoría personalizada de URL (**Objects [Objetos]** > **Custom Objects [Objetos personalizados]** > **URL Category [Categoría de URL]**) para limitar el alcance del tráfico que descifra. Cada regla de la política de descifrado usa la misma categoría personalizada de URL (y el mismo origen y destino) que la regla análoga de la política de seguridad, de modo que las políticas de descifrado y de seguridad se apliquen exactamente al mismo tráfico. La combinación de App-ID y una categoría personalizada de URL permite al cortafuegos descifrar solo el tráfico que la regla permite, lo que ahorra ciclos de procesamiento dado que no se descifrará el tráfico que el cortafuegos bloquee. (Se debe producir el descifrado antes de la evaluación de la regla de la política de seguridad).

STEP 1 | Descifre el tráfico entre los servidores del centro de datos y los servidores de actualización de software en internet.

En esta regla, se muestra cómo descifrar el tráfico de actualización de software del servidor del centro de datos para brindar visibilidad de las amenazas que pueden estar presentes en los servidores de actualización en internet, de modo que el cortafuegos pueda bloquearlas. En este ejemplo, se descifra el tráfico permitido entre los servidores del centro de datos y los servidores de actualización de CentOS en internet según la regla análoga de aplicaciones permitidas que se creó en Creación de reglas para aplicaciones permitidas desde el centro de datos hacia internet.

		Source		Destination			Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	ZONE	ADDRESS	URL CATEGORY	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
CentOS Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	CentOS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

Para crear esta regla:

- Especifique el mismo origen y destino que en la regla análoga de la política de seguridad. En este caso, el origen es el grupo de direcciones dinámicas **Dev-Servers** en la zona **Engineering-DC-Infra** y el destino es internet (zona **L3-External**).
- Especifique la misma categoría personalizada de URL que en la regla análoga de la política de seguridad (**CentOS-Update-Servers**) para limitar el alcance del descifrado a solo el tráfico que permite la regla, de modo que el cortafuegos no dedique ciclos a descifrar tráfico que eliminará.
- En la pestaña Options (Opciones), establezca la Action (Acción) como **Decrypt (Descifrar)** y el Type (Tipo) de descifrado como **SSL Forward Proxy (Proxy SSL de reenvío)**. Aplique el perfil de descifrado recomendado para el centro de datos para aplicar el proxy SSL de reenvío y los ajustes del protocolo SSL al tráfico.

Cree una regla similar en la política de descifrado para el tráfico del centro de datos que se permite en cada grupo de servidores del centro de datos que deba conectarse a servidores de actualización en internet, basada en el mismo origen y destino, y la misma categoría personalizada de URL que la regla análoga de la política de seguridad. Por ejemplo, la regla de la política de descifrado para los servidores del centro de datos que deben comunicarse con los servidores de actualización de Microsoft Windows, basada en la regla análoga de la política de seguridad, es la siguiente:

		Source		Destination			Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	ZONE	ADDRESS	URL CATEGORY	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Win Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	Win-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

STEP 2 | Descifre el tráfico entre los servidores del centro de datos y los servidores de actualización de NTP y DNS en internet.

En esta regla, se muestra cómo descifrar el tráfico de actualización de NTP y DNS del servidor del centro de datos para brindar visibilidad de las amenazas que pueden estar presentes en esos servidores de internet, de modo que el cortafuegos pueda bloquearlas. En este ejemplo, se descifra el tráfico permitido en función de la regla análoga de aplicaciones permitidas que se creó en Creación de reglas para aplicaciones permitidas desde el centro de datos hacia internet.

		Source		Destination			Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	ZONE	ADDRESS	URL CATEGORY	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
DNS-NTP Update Decrypt	DC to Internet BP	IT Infrastructure	DNS-NTP-Servers	L3-External	any	NTP-DNS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

Para crear esta regla:

- Especifique el mismo origen y destino que en la regla análoga de la política de seguridad. En este caso, el origen es el grupo de direcciones dinámicas **DNS-NTP-Servers** en la zona de la **IT Infrastructure (Infraestructura de TI)** y el destino es internet [zona **L3-External**].

- Especifique la misma categoría personalizada de URL que en la regla análoga de la política de seguridad (**NTP-DNS-Update-Servers**) para limitar el alcance del descifrado solo al tráfico que permite la regla.
- En la pestaña Options (Opciones), establezca la Action (Acción) como **Decrypt (Descifrar)** y el Type (Tipo) de descifrado como **SSL Forward Proxy (Proxy SSL de reenvío)**. Aplique el perfil de descifrado recomendado para el centro de datos para aplicar el proxy SSL de reenvío y los ajustes del protocolo SSL al tráfico.

Definición de la política de seguridad para el tráfico inicial en el centro de datos

El tráfico del centro de datos fluye entre servidores del centro de datos y niveles de aplicación. Es posible aceptar que todo lo que se encuentra dentro del centro de datos es fiable y no es necesario inspeccionar el tráfico. Sin embargo, si un atacante pone en riesgo un servidor del centro de datos y el tráfico entre los niveles de aplicación no atraviesa el cortafuegos, el atacante puede moverse lateralmente en el centro de datos hacia servidores críticos y descargar más malware, readaptar los servidores y filtrar datos usando aplicaciones legítimas que no se encuentran en el centro de datos, como sucedió en varias de las principales filtraciones en los últimos años.

La mejor defensa frente al malware que se establece en el centro de datos es proteger el tráfico con reglas de aplicaciones permitidas estrictas y específicas, e inspeccionar el tráfico con cortafuegos de última generación ubicados entre los niveles de aplicación.

Además, no permita aplicaciones desconocidas en el centro de datos. Es posible que las aplicaciones desconocidas indiquen que un adversario logró acceder al centro de datos. Cree aplicaciones personalizadas para las aplicaciones internas exclusivas, de modo que pueda identificarlas con App-ID aplicar seguridad al tráfico. Si no crea aplicaciones personalizadas para sus aplicaciones exclusivas, el cortafuegos las verá como tráfico unknown-tcp o unknown-udp. El problema es que el cortafuegos trata a las aplicaciones exclusivas de la misma manera en la que trata a otras aplicaciones desconocidas y debe bloquear las aplicaciones desconocidas debido a que pueden ser herramientas de un atacante. Si permite aplicaciones desconocidas en el centro de datos, es posible que lo entregue a un atacante.

En el caso de las aplicaciones comerciales desconocidas, puede enviar una solicitud *a Palo Alto Networks para crear un App-ID.*

Si posee políticas existentes de cancelación de aplicaciones que creó únicamente para definir los tiempos de espera personalizados de una sesión en un conjunto de puertos, convierta las políticas existentes de cancelación de aplicaciones en políticas basadas en la aplicación configurando los tiempos de espera de una sesión basados en el servicio para conservar el tiempo de espera personalizado de cada aplicación y migrar la regla a una regla basada en la aplicación. Las políticas de cancelación de aplicaciones se basan en los puertos. Cuando usa políticas de cancelación de aplicaciones para conservar los tiempos de espera personalizados de una sesión en un conjunto de puertos, pierde visibilidad de la aplicación respecto a esos flujos, de modo que no sabe ni controla las aplicaciones que usan los puertos. Los tiempos de espera de una sesión basados en el servicio logran tiempos de espera personalizados y conservan la visibilidad de la aplicación.

- Enfoque hacia la seguridad del tráfico en el centro de datos
- Creación de reglas de aplicaciones permitidas en el centro de datos
- Creación de reglas para la política de descifrado en el centro de datos

Enfoque hacia la seguridad del tráfico en el centro de datos

El enfoque heredado tradicional hacia la protección del tráfico horizontal entre los servidores del centro de datos expone los activos valiosos al riesgo, mientras que el enfoque recomendado protege sus activos valiosos.

El enfoque tradicional	Riesgo	El enfoque recomendado
No es necesario segmentar el tráfico que no cruza el perímetro	Un atacante que pone a cualquier servidor del centro de	Segmente el tráfico entre los niveles de aplicación mediante

El enfoque tradicional	Riesgo	El enfoque recomendado
del centro de datos, de modo que el tráfico entre los niveles de aplicación no debe pasar por la infraestructura de seguridad.	datos en riesgo puede moverse lateralmente a los servidores críticos del centro de datos y readaptarlos. Los atacantes en el centro de datos se pueden mover libremente sin temor a que los descubran.	reglas de permiso estrictas para evitar la comunicación innecesaria, reducir la superficie de ataque y evitar que un atacante se mueva lateralmente en el centro de datos. Registre y supervise las infracciones de la lista de permitidos.
El centro de datos está seguro dentro de una red fiable, de modo que no es urgente añadir parches a los servidores del centro de datos con rapidez.	Las vulnerabilidades permanecen activas por más tiempo y ofrecen vectores de ataque a los atacantes.	Instale parches en los servidores del centro de datos de manera oportuna para detener las vulnerabilidades. La creación de reglas de lista de permitidos en la política de seguridad le permite comprender qué se ejecuta en el centro de datos y dónde se ejecutan los servicios no actualizados.
Combine el bloqueo y las alertas de los perfiles de prevención de amenazas de varios proveedores.	Un conjunto de herramientas individuales ofrece brechas de seguridad a los atacantes y es posible que no funcionen adecuadamente.	El conjunto de herramientas de seguridad coordinada de Palo Alto Networks trabaja en conjunto para encender la seguridad y evitar ataques, e identificar malware desconocido que intente propagarse en los servidores del centro de datos.

Además:

- Cree una cuenta de servicio única para cada función. Por ejemplo, permita que únicamente las cuentas de servicio específicas repliquen buzones de correo electrónico de intercambio y permita que únicamente las cuentas de servicio específicas en los servidores web envíen consultas a las bases de datos de MySQL. No use una cuenta de servicio para ambas funciones.
- Supervise las cuentas de servicio.
- No permita cuentas de usuario habituales en el centro de datos.

Cuando pase de reglas basadas en el puerto a reglas basadas en la aplicación, en la base de reglas, ubique la regla basada en la aplicación sobre la regla basada en el puerto que reemplazará. Restablezca el contador de coincidencias de la regla de la política *de ambas reglas. Si el tráfico coincide con la regla basada en el puerto, el conteo de coincidencias de la regla de la política aumenta. Ajuste la regla basada en la aplicación hasta que no existan coincidencias entre el tráfico y la regla basada en el puerto durante un tiempo, y elimine la regla basada en el puerto.*

Creación de reglas de aplicaciones permitidas en el centro de datos

El tráfico del centro de datos a menudo consiste en tráfico de aplicaciones de varios niveles que fluye entre diferentes niveles de servidor para proporcionar servicios para aplicaciones como SharePoint, WordPress, aplicaciones internas propias, etc. La arquitectura de aplicaciones de varios niveles más común consta

de servidores web (nivel de presentación), servidores de aplicaciones (nivel de aplicación) y servidores de bases de datos (nivel de datos). La página Creación de una estrategia de segmentación de centro de datos proporciona directrices acerca de cómo ubicar cortafuegos entre los niveles de la aplicación y cómo segmentar un centro de datos.

La manera en la que trata al tráfico entre los servidores del centro de datos depende del tráfico. Para la mayoría del tráfico de aplicaciones, añada perfiles de prevención de amenazas a las reglas de permitidos de la política de seguridad para inspeccionar el tráfico. Por ejemplo, aplique siempre los perfiles de seguridad recomendados para proteger el tráfico entre la web, la aplicación y los niveles de servidor de las aplicaciones financieras, aplicaciones de desarrollo de ingeniería, etc. La excepción a la aplicación de perfiles de prevención contra amenazas es el tráfico de aplicaciones de gran volumen y poco valor como la replicación del buzón de correo electrónico y los flujos de copias de seguridad. Todavía permite el acceso a estas aplicaciones, pero dado que el cortafuegos ya ha inspeccionado el tráfico antes de que se vuelva a aplicar, aplicar perfiles de prevención contra amenazas consume ciclos de CPU del cortafuegos sin brindar valor adicional.

El perfil de seguridad de WildFire identifica el malware desconocido que intenta propagarse en los servidores del centro de datos para evitar la filtración de datos descubriendo el malware antes de que haga daño. Si no puede usar la nube global de WildFire, puede implementar una nube privada de WildFire o una nube híbrida de WildFire.

Los ejemplos de reglas de la política de seguridad en esta sección muestran cómo permitir el tráfico de aplicaciones de finanzas de varios niveles en el centro de datos que requieren el uso de niveles de servidor web, servidor de aplicación y servidor de base de datos para atender a las aplicaciones. El ejemplo incluye dos aplicaciones internas exclusivas para las que se crearon aplicaciones personalizadas: **Billing-App** y **Payment-App**. Crear App-ID personalizados para estas aplicaciones permite que el cortafuegos las identifique, las controle y les aplique una política de seguridad. No permita aplicaciones desconocidas en el centro de datos dado que no puede identificarlas y aplicarles seguridad, y es posible que indiquen que existe un adversario en el centro de datos. Cada aplicación en el centro de datos debe tener un App-ID.

Permita las aplicaciones únicamente en sus puertos estándar (application-default). En algunos casos, es posible que las necesidades empresariales requieran que haga una excepción y permita aplicaciones que usan puertos no estándar entre determinados clientes y servidores. En estos casos, tenga en cuenta el tráfico de aplicación que se ejecuta en puertos no estándar y asegúrese de conocer cada instancia de una aplicación que se ejecuta en un puerto no estándar. Es posible que las aplicaciones que se ejecutan en puertos no estándar para las que no crearon excepciones explícitas (conocidas) indiquen la presencia de malware evasivo.

Etiquete todas las aplicaciones sancionadas *con la etiqueta Sanctioned (Sancionado) predefinida. Panorama y los cortafuegos consideran a las aplicaciones sin la etiqueta Sanctioned (Sancionado) como aplicaciones no sancionadas.*

Orden de la base de reglas de la política de seguridad del centro de datos le muestra cómo ordenar estas reglas con todas las otras reglas que creamos para los otros tres flujos de tráfico en el centro de datos y las reglas de bloqueo, de modo que ninguna regla enmascareque a otra.

Para aplicar una política de seguridad uniforme en varios centros de datos, puede reusar las plantillas y las pilas de plantillas, de modo que las mismas políticas se apliquen en cada centro de datos. Las plantillas usan variables para aplicar valores para dispositivos

específicos como direcciones IP, FQDN, etc., conservar una política de seguridad global y reducir el número de plantillas y pilas de plantillas que debe gestionar.

Cada una de las siguientes reglas de permiso:

- Tiene la práctica recomendada grupo de perfiles de seguridad adjunta, que consta de los perfiles de seguridad de práctica recomendada. El uso de un grupo de perfiles de seguridad le permite aplicar todos los perfiles de prácticas recomendadas a una regla a la vez en lugar de especificar cada perfil individualmente. Los grupos de perfiles de seguridad hacen que la configuración de la protección contra malware, vulnerabilidades, tráfico C2 y amenazas conocidas y desconocidas sea más rápida y sencilla.
- Registra el tráfico (al final de la sesión) para que pueda realizar un seguimiento y analizar las infracciones de las reglas, e incluye el reenvío de logs. Reenvíe los logs a los servidores de logs y, cuando corresponda, reenvíe los correos electrónicos de logs a los administradores correspondientes.

STEP 1 | Permita el tráfico de la aplicación de finanzas entre el nivel de servidor web y el nivel de servidor de la aplicación.

Esta regla limita el tráfico que puede fluir entre el nivel de servidor web y el nivel de servidor de la aplicación en los servidores de facturación del departamento de finanzas, de modo que solo el tráfico que use aplicaciones legítimas pueda acceder a los servidores de facturación. (También se ha creado un regla para limitar el acceso de los usuarios de finanzas al centro de datos cuando se llevo a cabo la Creación de reglas de aplicaciones permitidas desde el usuario al centro de datos, de modo que únicamente los usuarios de finanzas adecuados puedan acceder al centro de datos). La regla usa grupos de direcciones dinámicas para especificar los servidores en cada nivel de aplicación; **Web-Servers** especifica las direcciones de los servidores en el nivel de servidor web y **Billing-App-Servers** especifica las direcciones de los servidores en el nivel de servidor de la aplicación de facturación de finanzas.

			Source			Destination						
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Web to App Server	Intra DC BP	universal	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	Billing-App Payment-App ssl web-browsing	application-default	Allow		

Para crear esta regla:

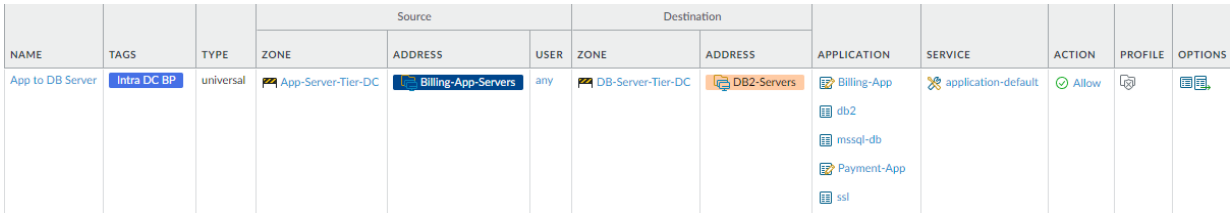
- Limite el origen del tráfico de la aplicación de finanzas a los servidores web (**Web-Servers**) en la zona **Web-Server-Tier-DC**.
- Limite el destino del tráfico de la aplicación de finanzas a los servidores de facturación (**Billing-App-Servers**) en la zona **App-Server-Tier-DC**.
- Limite las aplicaciones que pueden usar los servidores web para acceder a los servidores de la aplicación de facturación y permita únicamente las aplicaciones en sus puertos predeterminados. En este ejemplo, las aplicaciones incluyen dos aplicaciones personalizadas, **Billing-App** y **Payment-App**, para las que especifica puertos predeterminados cuando crea las aplicaciones. El departamento de finanzas usa estas aplicaciones exclusivas para los servicios de facturación y pago.

Cree reglas similares para controlar aplicaciones y el tráfico entre el nivel de servidor web y otros niveles de servidor de la aplicación.

STEP 2 | Permita el tráfico de la aplicación de finanzas entre el nivel de servidor de la aplicación y el nivel de servidor de la base de datos.

Esta regla limita el tráfico que puede fluir entre el nivel de servidor de la aplicación y el nivel de servidor de la base de datos en los servidores de facturación del departamento de finanzas, de modo que solo el tráfico que use aplicaciones legítimas puede fluir entre los servidores de la aplicación de facturación y los servidores de la base de datos de facturación. La regla usa grupos de direcciones dinámicas para especificar los servidores en cada nivel de aplicación; **Billing-App-Servers** especifica las direcciones de

los servidores en el nivel de servidor de la aplicación y **DB2-Servers** especifica las direcciones de los servidores en el nivel de servidor de la base de datos de finanzas.



Para crear esta regla:

- Limite el origen del tráfico de la aplicación de finanzas a los servidores de la aplicación de facturación (**Billing-App-Servers**) en la zona **App-Server-Tier-DC**.
- Limite el destino del tráfico de la aplicación de finanzas a los servidores de la base de datos (**DB2-Servers**) en la zona **DB-Server-Tier-DC**.
- Limite las aplicaciones que pueden usar los servidores de la aplicación de facturación para acceder a los servidores de la base de datos y permita únicamente las aplicaciones en los puertos predeterminados o los puertos no predeterminados conocidos.

Cree reglas similares para controlar aplicaciones y el tráfico entre el nivel de servidor de la aplicación y el nivel de servidor de la base de datos de otras aplicaciones.

Verifique que solo se ejecuten las aplicaciones que permitió explícitamente en las reglas de la política de seguridad viendo el informe de aplicaciones predefinido [**Monitor (Supervisar)** > **Reports (Informes)** > **Application Reports (Informes de aplicación)** > **Applications (Aplicaciones)**]. Si ve aplicaciones inesperadas en el informe, revise las reglas de aplicaciones permitidas y vuelva a ajustarlas, de modo que no permitan aplicaciones inesperadas.

Creación de reglas para la política de descifrado en el centro de datos

¿Por qué descifrar el tráfico dentro del centro de datos? Después de todo, no hay usuarios y el centro de datos es un entorno seguro dentro de la red segura. Pero nada podría ser más erróneo. El centro de datos es una ubicación ideal para que se oculten los atacantes, precisamente, debido a que muchas personas creen que el centro de datos es seguro y no lo examinan. Pero el mismo principio que se aplica al resto de las redes se aplica al centro de datos: no puede protegerse de lo que no puede ver. Descifre el tráfico cifrado del centro de datos, de modo que el cortafuegos pueda inspeccionarlo, controlar el acceso, hacer visibles las amenazas y proteger los activos valiosos.

Existe tráfico en el centro de datos que no está cifrado (texto no cifrado). No habilite el descifrado de flujos de texto no cifrado debido a que no hay tráfico para descifrar.

En Creación de reglas de aplicaciones permitidas en el centro de datos, se crearon reglas en la política de seguridad que permiten que los servidores involucrados con aplicaciones del departamento de finanzas en diferentes niveles de la aplicación se comuniquen entre sí. A continuación, crearemos reglas análogas en la política de descifrado para descifrar el tráfico que permiten esas reglas.

Para cada regla, configure el registro de descifrado y reenvío de logs. Registre tanto tráfico de descifrado como lo permitan los recursos de su cortafuegos.

STEP 1 | Descifre el tráfico de la aplicación de finanzas entre el nivel de servidor web y el nivel de servidor de la aplicación.

Esta regla descifra el tráfico que fluye entre el nivel de servidor web y el nivel de servidor de la aplicación para los servidores de facturación del departamento de finanzas, de modo que el cortafuegos pueda ver el tráfico y proteger a los servidores en cada nivel contra las posibles amenazas.

		Source			Destination		Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Web to App	Intra DC BP	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

Para crear esta regla:

- Especifique el mismo origen y destino que en la regla análoga de la política de seguridad. En este ejemplo, el origen es el grupo de direcciones dinámicas de los **Web-Servers** en la zona **Web-Server-Tier-DC** y el destino son los **Billing-App-Servers** en la zona **App-Server-Tier-DC**.
- En la pestaña Options (Opciones), establezca la Action (Acción) como **Decrypt (Descifrar)** y el Type (Tipo) de descifrado como **SSL Forward Proxy (Proxy SSL de reenvío)**. Aplique el perfil de descifrado recomendado para el centro de datos para aplicar el proxy SSL de reenvío y los ajustes del protocolo SSL al tráfico.

STEP 2 | Descifre el tráfico de la aplicación de finanzas entre el nivel de servidor de la aplicación y el nivel de servidor de la base de datos.

Esta regla descifra el tráfico que fluye entre el nivel de servidor de la aplicación y el nivel de servidor de la base de datos para los servidores de facturación del departamento de finanzas, de modo que el cortafuegos pueda ver el tráfico y proteger a los servidores en cada nivel contra las posibles amenazas.

		Source			Destination		Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
App to DB	Intra DC BP	App-Server-Tier-DC	Billing-App-Servers	any	DB-Server-Tier-DC	DB2-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

Para crear esta regla:

- Especifique el mismo origen y destino que en la regla análoga de la política de seguridad. En este ejemplo, el origen es el grupo de direcciones dinámicas de los **Billing-App-Servers** en la zona **App-Server-Tier-DC** y el destino son los **DB2-Servers** en la zona **DB-Server-Tier-DC**.
- En la pestaña Options (Opciones), establezca la Action (Acción) como **Decrypt (Descifrar)** y el Type (Tipo) de descifrado como **SSL Forward Proxy (Proxy SSL de reenvío)**. Aplique el perfil de descifrado recomendado para el centro de datos para aplicar el proxy SSL de reenvío y los ajustes del protocolo SSL al tráfico.

Orden de la base de reglas de la política de seguridad del centro de datos

Este tema proporciona un resumen de la base de reglas de la política de seguridad de ejemplo que muestra el orden de las reglas para los cuatro flujos de tráfico del centro de datos. Las secciones anteriores analizan cada regla en la política de seguridad en detalle (así como las reglas en la política de descifrado, y cuando sea necesario, las reglas en la política de autenticación y en la política de protección contra DoS).

El orden de las reglas de la política de seguridad es fundamental. Ninguna regla debe enmascarar a otra regla. Por ejemplo, las reglas de bloqueo no deben bloquear el tráfico que desea permitir, por lo que debe colocar las reglas de permiso *antes* de que la regla que bloqueo del tráfico entre en vigor. Además, una regla de permiso no deberá permitir el tráfico que desea bloquear. Al crear reglas de permisos muy específicas, controla estrictamente las aplicaciones permitidas y quién puede y quién no puede usarlas.

Reglas 1-7: Las dos primeras reglas bloquean la aplicación QUIC para evitar que bloquee el tráfico o impida el descifrado. Las siguientes cinco reglas permiten el acceso al DNS para los usuarios y permiten el acceso a aplicaciones y servidores específicos para grupos de usuarios específicos. Estas son las reglas configuradas en Creación de reglas de aplicaciones permitidas desde el usuario al centro de datos.

			Source			Destination						
	NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
1	Block QUIC UDP	none	any	any	any	L3-External	any	any	quic_udp_ports	Deny	none	
2	Block QUIC	none	any	any	any	L3-External	any	quic	application-default	Deny	none	
3	DNS Services	User to DC BP	any	any	any	IT Infrastructure	DNS-Servers	dns	application-default	Allow		
4	IT DC Server Management	User to DC BP	IT-Users	any	it-superusers	IT-Server-Access-DC	IT-Server-Management	ms-rdp ssh ssl	Custom-IT-Ports	Allow		
5	Engineering Resources	User to DC BP	Engineering-Users	any	api-users engg-users	Engineering-DC-Infra	Dev-Servers	oracle-bi perforce profinet qlikview	application-default	Allow		
6	Finance to DC	User to DC BP	Finance-Users	any	accounting-users finance-users	Finance-DC-Infra	Fin-Servers	netsuite oracle oracle-crm-ondemand oracle-forms	application-default	Allow		
7	SAP-Contractors	User to DC BP	Contractors	any	sap-contractors	SAP-Infra	SAP DB Servers	ms-sql-analysis-service mssql-db mssql-mon sap	application-default	Allow		

Figure 1: Reglas 1-7 del centro de datos

Solo los usuarios especificados pueden usar las aplicaciones especificadas en sus puertos predeterminados para acceder únicamente a los servidores de destino (direcciones) del centro de datos especificado. Los perfiles de seguridad protegen todas las reglas de permiso contra amenazas. Estas reglas se encuentran antes de las reglas de bloqueo que descubren usuarios y aplicaciones no conocidos en la red debido a que estas reglas son muy específicas y evitan que usuarios y aplicaciones autorizados coincidan con reglas más generales más abajo en la base de reglas.

Reglas 8-9: Si bien las reglas anteriores permiten aplicaciones autorizadas, las dos siguientes reglas, creadas en Creación de reglas de bloqueo de tráfico en el centro de datos, descubren y bloquean aplicaciones inesperadas de usuarios en puertos estándar y bloquean todas las aplicaciones en puertos no estándar. (Su implementación puede tener más zonas de usuario de las que se muestran en el ejemplo).

	NAME	TAGS	Source			Destination		APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	ZONE	ADDRESS					
8	Unexpected-App-from-User-Zone	User to DC BP	Contractors Engineering-Users Finance-Users IT-Users	any	any	Web-Server-Tier-DC	any	any	application-default	Drop	none	
9	Unexpected-User-App-Any-Port	User to DC BP	Contractors Engineering-Users Finance-Users IT-Users	any	any	Web-Server-Tier-DC	any	any	any	Drop	none	

Figure 2: Reglas del centro de datos 8-9

El tráfico de zonas de no usuarios no coincide con estas reglas. Coloque estas reglas por encima de las reglas de bloqueo de aplicaciones (reglas 18 y 19) o esas reglas harán sombra a estas reglas. (Es posible que el tráfico que coincide con estas dos reglas también coincida con reglas de bloqueo de aplicaciones más general. Si las reglas de bloqueo de aplicaciones se encuentran en primer lugar y coinciden con el tráfico que también coincide con estas reglas, ese tráfico no coincidirá con estas reglas y no se registrará por separado, por lo que las reglas no realizarán su función prevista de diferenciar el bloqueo que resulta de la actividad de usuarios empleados del bloqueo causado por la actividad de otras zonas).

Reglas 10-16: Las siguientes siete reglas permiten el tráfico entre el centro de datos e Internet y dentro del centro de datos (creado en Creación de reglas de aplicaciones permitidas desde internet al hacia centro de datos, Creación de reglas para aplicaciones permitidas desde el centro de datos hacia internet y Creación de reglas de aplicaciones permitidas en el centro de datos). Los perfiles de seguridad protegen todas las reglas de permiso contra amenazas.

	NAME	TAGS	Source			Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	ZONE	ADDRESS						
10	Web Server Inbound	Internet to DC BP	L3-External	~~Bad IPs List~~	any	Web-Server-Tier-DC	Web Servers	Acme	application-default	any	Allow		
11	NTP DNS Update	DC to Internet BP	IT Infrastructure	DNS-NTP-Servers	any	L3-External	any	dns ntp	application-default	NTP-DNS-Update-Servers	Allow		
12	CentOS Update	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	yum	application-default	CentOS-Update-Servers	Allow		
13	Windows Update	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	ms-update ssl	application-default	Win-Update-Servers	Allow		
14	Cert Update	DC to Internet BP	IT Infrastructure	IT-Server-Management	any	L3-External	any	ocsp	application-default	any	Allow		
15	App to DB Server	Intra DC BP	App-Server-Tier-DC	Billing-App-Servers	any	DB-Server-Tier-DC	DB2-Servers	Billing-App db2 mssql-db Payment-App ssl	application-default	any	Allow		
16	Web to App Server	Intra DC BP	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	Billing-App Payment-App ssl web-browsing	application-default	any	Allow		

Figure 3: Reglas de centro de datos 10-16

Reglas 17-20: Las últimas cuatro reglas, que se configuraron en Creación de reglas de bloqueo de tráfico en el centro de datos, bloquean las aplicaciones que no desea en su centro de datos y las aplicaciones inesperadas, y descubren usuarios no previstos en su red.

		Source			Destination						
	NAME	ZO...	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
17	Block-Bad-Apps	any	any	any	App-Server-Tier-DC DB-Server-Tier-DC Engineering-DC-Infra Finance-DC-Infra IT Infrastructure SAP-Infra Web-Server-Tier-DC	any	Encrypted-Tunnels File-Sharing Remote-Access	any	Drop	none	
18	Unexpected-App-from-Any-Zone	any	any	any	Web-Server-Tier-DC	any	any	application-default	Drop	none	
19	Unexpected-App-Any-Port	any	any	any	Web-Server-Tier-DC	any	any	any	Drop	none	
20	Discover-Unknown-Users	any	any	unknown	any	any	any	any	Deny	none	

La regla 17 bloquea las aplicaciones que no desea nunca en su centro de datos. Esta regla viene después de las reglas de aplicaciones permitidas para habilitar el acceso para excepciones. Por ejemplo, puede autorizar una o más aplicaciones de uso compartido de archivos en las reglas de aplicaciones permitidas anteriores a esta regla de bloqueo, y el filtro de aplicaciones en esta regla bloqueará el resto de los tipos de aplicaciones para evitar el uso de aplicaciones de uso compartido de archivos no sancionadas. Si existen conjuntos de aplicaciones o aplicaciones individuales que no desea en la red y para las que no hay excepciones, por ejemplo, BitTorrent, puede crear una regla de bloqueo específica para bloquear esas aplicaciones y colocarlas en la parte superior de la base de reglas, sobre las reglas de aplicaciones permitidas. Sin embargo, si hace esto, debe asegurarse de que ninguna de las aplicaciones bloqueadas tenga usos comerciales legítimos porque sus usuarios no podrán acceder a ellas.

Las reglas 18 y 19 son análogas a las reglas 8 y 9, que descubren aplicaciones inesperadas de usuarios (el tráfico al que se aplican estas reglas proviene únicamente de zonas de usuarios). Las reglas 18 y 19 descubren aplicaciones inesperadas del resto de las zonas. Las reglas separadas le permiten registrar las coincidencias de la regla de bloqueo con mayor detalle.

La regla 20 descubre usuarios desconocidos, de modo que pueda registrar esos intentos de acceso por separado para facilitar la investigación.

Al igual que en todas las bases de reglas en la política de seguridad, las últimas dos reglas serán reglas predeterminadas de Palo Alto Networks para el tráfico de la intrazona (permiso) y el tráfico de la interzona (bloqueo).

Registro y supervisión del tráfico de centro de datos

Las herramientas de generación de logs y supervisión del cortafuegos revelan aplicaciones, usuarios y patrones de tráfico en la red, como aplicaciones y usuarios que quizás no sabía que estaban allí. La creación de logs y la supervisión brinda información útil en todas las etapas de la transición y el mantenimiento de una política de seguridad recomendada para el centro de datos debido a que revela usuarios desconocidos (no identificados con User-ID), aplicaciones desconocidas y tráfico en puertos inesperados, lo que indica que una regla en la política de seguridad no se desarrolló correcta o estrictamente. La creación de logs y la supervisión de información le permiten determinar qué aplicaciones permitir y a quienes permitir el acceso a determinadas aplicaciones y dispositivos, y también ayuda a investigar posibles problemas de seguridad.

Cuando evalúa el centro de datos, captura mediciones de referencia. Compare periódicamente esas mediciones de referencia con las mediciones actuales para evaluar el progreso, identificar cambios y descubrir áreas de mejora a medida que implementa la política de seguridad recomendada para el centro de datos.

Si usa Panorama para gestionar los cortafuegos, puede supervisar el estado del cortafuegos para comparar los dispositivos con el rendimiento de referencia y entre sí para identificar las desviaciones del comportamiento normal.

Configure el reenvío de logs desde los cortafuegos hacia Panorama o hacia servicios externos, como un servidor de capturas de SNMP o un servidor syslog para centralizar los logs de varios cortafuegos a fin de visualizarlos y analizarlos de manera más conveniente (un cortafuegos solo puede mostrar los logs y los informes locales, no los de otros cortafuegos). Cuando configure el reenvío de logs, configure el envío de notificaciones para verificar que los destinos de los logs que configuró reciban los logs del cortafuegos.

Las prácticas recomendadas de generación de logs y supervisión para el centro de datos incluyen las siguientes:

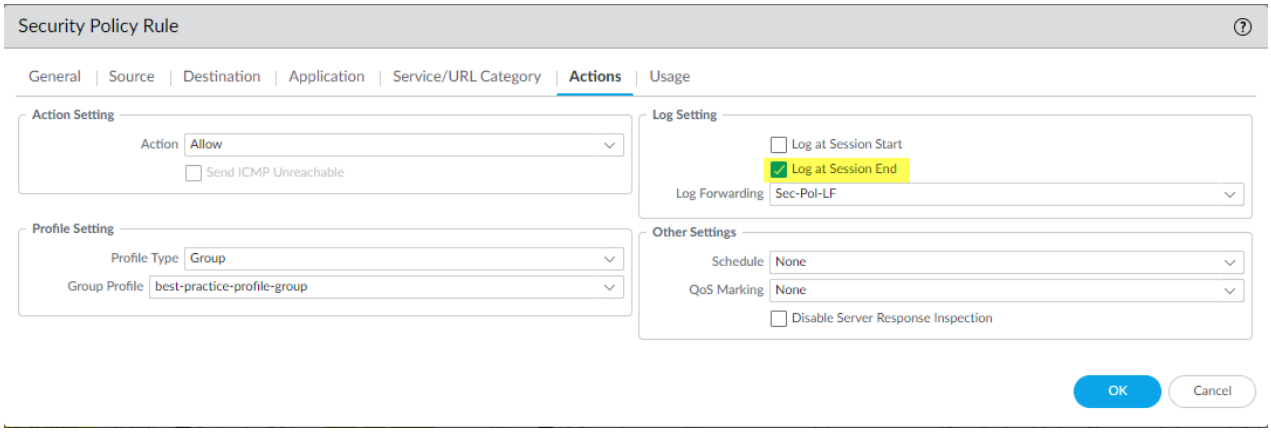
- Tráfico del centro de datos que registrar y supervisar
- Supervisión de las reglas de bloqueo para el centro de datos y ajuste de la base de reglas
- Registro del tráfico en el centro de datos que no coincide con reglas en la interzona
- Registro del tráfico en el centro de datos que coincide con las reglas de permiso en la intrazona

Tráfico del centro de datos que registrar y supervisar

El cortafuegos de última generación de Palo Alto Networks crea algunos registros de manera predeterminada y debe configurar la creación de logs para otro tráfico. Se recomienda registrar todo el tráfico del centro de datos y supervisar los logs de aplicaciones, usuarios, tráfico y comportamientos inesperados.

De manera predeterminada, el cortafuegos registra el tráfico que coincide con las reglas en la política de seguridad que se configuran explícitamente y no registra el tráfico que coincide con las reglas predefinidas intrazone-default (intrazona-predeterminada) (que permite tráfico con un origen y un destino en la misma zona) e interzone-default (interzona-predeterminada) (la última regla en la base de reglas, que bloquea el tráfico que coincide con las reglas anteriores) en la parte inferior de la base de reglas.

Cuando crea una regla de política de seguridad, el cortafuegos registra el tráfico al final de la sesión de forma predeterminada:



Sin embargo, el cortafuegos no reenvía logs de forma predeterminada ni aplica perfiles de seguridad, de forma predeterminada. El ejemplo anterior muestra la práctica recomendada de reenviar logs a los administradores y servidores de registro adecuados y aplicar los perfiles de seguridad de las prácticas recomendadas.

Para la mayor parte del tráfico, se recomienda seleccionar **Log at Session End (Log al finalizar sesión)** debido a que las aplicaciones cambian frecuentemente durante una sesión. Por ejemplo, es posible que el App-ID inicial de una sesión sea web-browsing (navegación web), pero después de procesar algunos paquetes, el cortafuegos puede hallar App-ID más específicos para la aplicación y cambiarlo. Existen varios casos de uso de la generación de logs de tráfico al inicio de la sesión, que incluye sinkhole DNS, sesiones de túnel prolongadas y cuando necesita información del inicio de la sesión para solucionar problemas.

Generar logs del tráfico permite registrar información sobre el tráfico que permite una regla y el tráfico que bloquea o elimina (incumplimientos a la regla) una regla, de modo que el cortafuegos brinde información valiosa independientemente de cómo trate al tráfico. Los incumplimientos de las reglas destacan posibles ataques o reglas de permiso que deben ajustarse para permitir una aplicación empresarial legítima.

Cuando examine el tráfico bloqueado en los logs, diferencie el tráfico que el cortafuegos bloqueó como protección antes de que los sistemas se encontraran en riesgo, como el bloqueo de una aplicación que no está permitida, y el tráfico que bloqueó tras un evento de riesgo, por ejemplo, el intento de un malware que ya se encuentra en el servidor de un centro de datos de comunicarse con un servidor externo para descargar malware o filtrar datos.

El cortafuegos brinda una variedad de herramientas de supervisión, logs e informes de logs para analizar su red:

- **Monitor (Supervisar)** > **Logs** ofrece logs de tráfico, amenazas, User-ID, y otros tipos de logs, como los logs **Unified (Unificados)**, que muestran varios tipos de logs en una pantalla, de modo que no deba ver diferentes tipos de logs por separado. Cuando se incluye un icono de lupa en el resumen, puede hacer clic en él para acceder a la entrada del log.
- **Monitor (Supervisar)** > **PDF Reports (Informes en PDF)** ofrece informes predefinidos que puede ver y la capacidad de crear grupos de informes con informes predefinidos y personalizados. Por ejemplo, puede revisar la actividad del tráfico o tomar mediciones de referencia para comprender el uso del ancho de banda y el flujo de tráfico en cada segmento del centro de datos por zona o interfaz.
- **Monitor (Supervisar)** > **Manage Custom Reports (Gestionar informes personalizados)** ofrece la capacidad de crear informes personalizados, de modo que pueda ver información sobre las reglas de bloqueo, las reglas de permiso u otro tema de interés.
- **Monitor (Supervisar)** > **Packet Capture (Captura de paquetes)** le permite realizar captura de paquetes del tráfico que atraviesa la interfaz de gestión y la interfaz de red del cortafuegos.
- El Centro de control de aplicaciones (**Application Command Center, ACC**) ofrece widgets que muestran un resumen interactivo y gráfico de las aplicaciones, los usuarios, las URL, las amenazas y el contenido

que atraviesan la red. Por ejemplo, puede revisar y evaluar las aplicaciones en la red [**ACC** > **Network Activity (Actividad de la red)** > **Application Usage (Uso de la aplicación)** > **Threats (Amenazas)**] para ver si se produjeron cambios en la aplicación o si la aplicación presenta el comportamiento de una amenaza. Si ve aplicaciones inesperadas en la lista, evalúe cómo manejarlas.

Otra buena manera de usar información del ACC es ayudar a identificar cuentas de usuario y sistemas de host en riesgo. Analice las amenazas junto con los nombres de usuario asociados a las amenazas usando el widget **ACC** > **Network Activity (Actividad de red)** > **User Activity (Actividad de usuarios)** > **Threats (Amenazas)** y use los logs de amenazas para aislar el problema exacto.

- El panel [**Dashboard (Panel)**] ofrece widgets que muestran la información general del cortafuegos y hasta 10 de las entradas más recientes de logs de amenazas, configuración y sistema.
- Use Panorama para supervisar el estado del cortafuegos y recopilar información de referencia para los dispositivos nuevos; comparar las métricas de rendimiento; y realizar un seguimiento del rendimiento del cortafuegos tras un evento, como de confirmación, una actualización de software, actualizaciones de contenido, cambios en las reglas, la incorporación de aplicaciones nuevas, etc. Si el rendimiento es diferente al del valor de referencia de un dispositivo, podrá ver y solucionar el problema manualmente, o crear automáticamente una incidencia para investigación.
- En Panorama o en un cortafuegos individual, use el contador de coincidencias de la regla de la política para analizar los cambios en la base de reglas. Por ejemplo, cuando añade una aplicación nueva, antes de permitir el tráfico de la aplicación en la red, añada la regla de permiso en la base de reglas. Si el tráfico coincide con la regla y aumenta el valor del contador, indica que es posible que el tráfico que coincide con la regla ya se encuentre en la red incluso si aún no activó la aplicación o que debe ajustar la red. Otro ejemplo es reemplazar las reglas basadas en el puerto con reglas basadas en la aplicación ubicando la regla basada en la aplicación antes de la regla basada en el puerto y comprobar si el tráfico coincide con la regla basada en el puerto. Si el tráfico coincide con la regla basada en el puerto, debe ajustar la regla basada en la aplicación para que capture ese tráfico.

  En combinación con el contador de coincidencias de la regla de la política, compruebe los widgets **ACC** > **Threat Activity (Actividad de amenazas)** > **Applications Using Non Standard Ports (Aplicaciones que usan puertos no estándar)** y **ACC** > **Threat Activity (Actividad de amenazas)** > **Rules Allowing Apps On Non Standard Ports (Reglas que permiten aplicaciones en puertos no estándar)** para verificar si el tráfico en puertos no estándar provocó las coincidencias inesperadas con la regla.

  La clave para usar el contador de coincidencias de la regla de la política es restablecer el contador cuando realiza un cambio, como la introducción de una nueva aplicación o el cambio del significado de una regla. Restablecer el contador garantiza que verá el resultado del cambio, no resultados que incluyen el cambio y los eventos que se produjeron antes del cambio.

Supervisión de las reglas de bloqueo para el centro de datos y ajuste de la base de reglas

El desarrollo de una política de seguridad recomendada es un proceso iterativo. En cuanto cree reglas de bloqueo de tráfico en el centro de datos, comience a supervisar el tráfico que coincide con las reglas de bloqueo diseñadas para identificar brechas en la política, comportamientos inesperados y posibles ataques. Ajuste las reglas de aplicaciones permitidas para tener en cuenta el tráfico que coincide con las reglas de bloqueo, pero que debería permitirse e investigue el tráfico que podría indicar un ataque.

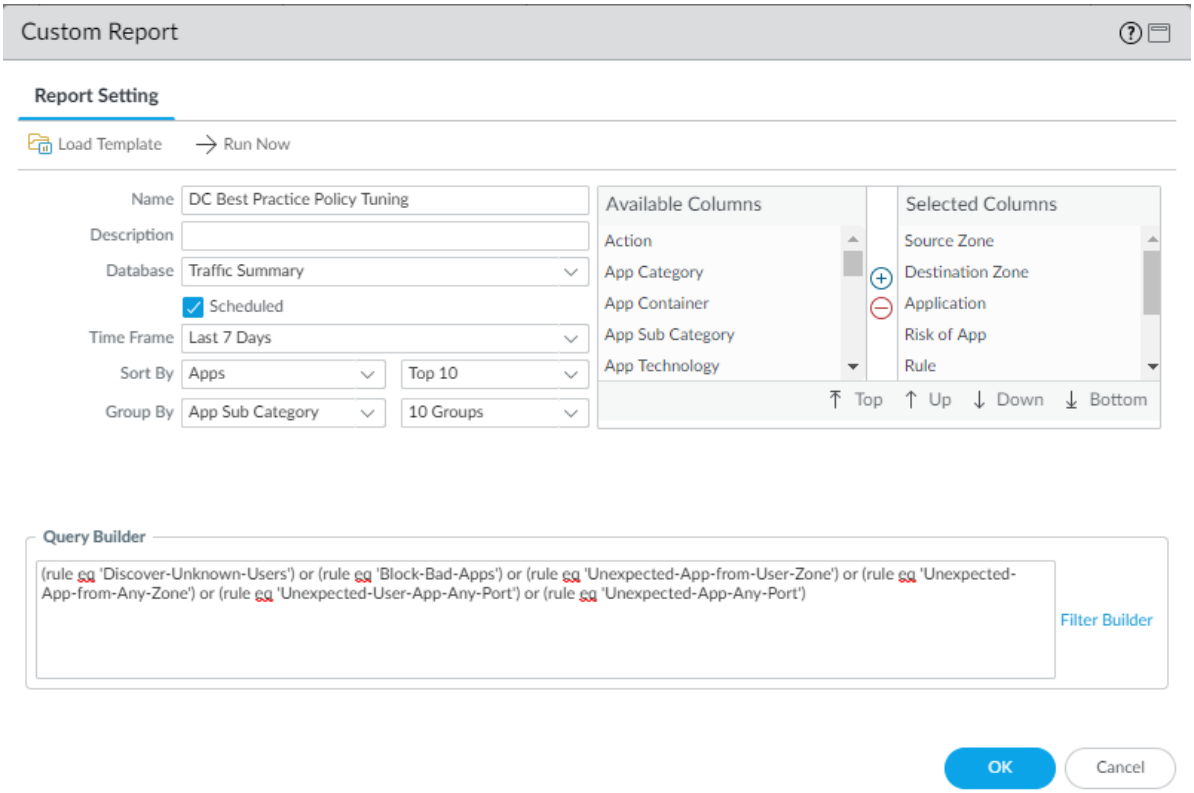
Los informes del tráfico bloqueado incluyen información valiosa que puede usar para investigar posibles problemas. Mantenga las reglas de bloqueo en la base de reglas para proteger sus activos valiosos en el centro de datos y que brinde esa información cuando el tráfico coincide con una regla de bloqueo.

Respete las prácticas recomendadas para las actualizaciones de contenido a fin de mantener actualizada la protección del cortafuegos. Mantenimiento de la base de reglas recomendadas

para el centro dedatos *incluye prácticas recomendadas específicas para los cortafuegos del centro de datos.*

STEP 1 | Cree informes personalizados para supervisar tráfico que coincida con las reglas de bloqueo diseñadas para identificar las brechas de la política y posibles ataques.

1. Seleccione **Monitor (Supervisar)** > **Manage Custom Reports (Gestionar informes personalizados)**.
2. Haga clic en **Add (Añadir)** para añadir un informe y asígnele un **Name (Nombre)** que describa el propósito del informe, en este ejemplo, **DC Best Practice Policy Tuning (Ajuste de la política recomendada para el centro de datos)**.
3. Configure la **Database (Base de datos)** en **Traffic Summary (Resumen de tráfico)**. Esto también cambia las opciones de **Available Columns (Columnas disponibles)**.
4. De **Available Columns (Columnas disponibles)**, añada **Source Zone (Zona de origen)**, **Destination Zone (Zona de destino)**, **Sessions (Sesiones)**, **Bytes**, **Application (Aplicación)**, **Risk of App (Riesgo de la aplicación)**, **Rule (Regla)** y **Threats (Amenazas)** a la lista **Selected Columns (Columnas seleccionadas)**. Si desea supervisar otros tipos de información, selecciónelos.
5. Seleccione la casilla de verificación **Scheduled (Programado)**.
6. Configure los valores de **Time Frame (Periodo)**, **Sort By (Ordenar por)** y **Group By (Agrupar por)** que desee. En este ejemplo, establecemos el **Time Frame (Período de tiempo)** en **Last 7 Days (Últimos 7 días)**, el **Sort By (Ordenar por)** en **Apps (Aplicaciones)** y el **Group by (Agrupar)** en **App Sub Category (Subcategoría de aplicaciones)**.
7. Defina la consulta para buscar el tráfico que coincida con las reglas diseñadas para detectar brechas de la política y posibles ataques. Puede crear un solo informe del tráfico que coincide con cualquiera de las reglas usando el operador **or** o crear informes individuales para supervisar cada regla. En **Query Builder (Generador de consultas)**, especifique el nombre de cada regla que desee incluir en el informe. Este ejemplo usa las seis reglas de bloqueo y usa el operador **Or** para incluir información sobre el tráfico que coincide con cualquiera de las reglas:
   - `(rule eq 'Discover-Unknown-Users')`
   - `(rule eq 'Block-Bad-Apps')`
   - `(rule eq 'Unexpected-App-from-User-Zone')`
   - `(rule eq 'Unexpected-App-from-Any-Zone')`
   - `(rule eq 'Unexpected-User-App-Any-Port')`
   - `(rule eq 'Unexpected-App-Any-Port')`



STEP 2 | Revise el informe (o informes) periódicamente para asegurarse de que comprende por qué el tráfico coincide con cada una de las reglas de bloqueo y actualice la política para incluir aplicaciones y usuarios legítimos, o use la información para evaluar el riesgo del tráfico que coincide con las reglas.

Registro del tráfico en el centro de datos que coincide con las reglas de permiso en la intrazona

De manera predeterminada, se permite todo el tráfico de intrazona (origen y destino en la misma zona). Después de que el cortafuegos evalúa la política de seguridad, permite el tráfico que controla las reglas de aplicaciones permitidas, bloquea el tráfico que controlan las reglas de bloqueo, o si el tráfico de intrazona no coincide con ninguna regla, el cortafuegos lo permite de manera predeterminada. (El cortafuegos bloquea el tráfico de interzona de manera predeterminada). Debido a la naturaleza valiosa de los activos del centro de datos, se recomienda supervisar todo el tráfico en el centro de datos entre los servidores del centro de datos, que incluye el tráfico que permite la regla de permiso de intrazona predeterminada.

Para obtener visibilidad del tráfico, habilite la generación de logs en la regla intrazone-default (intrazona-predeterminada) cuando se aplica al tráfico entre las zonas dentro del centro de datos. Registrar el tráfico permite examinar el acceso que no permitió explícitamente y que es posible que desee permitir explícitamente modificando una regla de permiso o un regla de bloqueo explícito.

En Definición de la política de seguridad para el tráfico inicial en el centro de datos, se usaron tres ejemplos de zonas en el centro de datos: Web-Server-Tier-DC, App-Server-Tier-DC y DB-Server-Tier-DC. En este ejemplo, se crea un informe personalizado para recopilar información de logs sobre el tráfico de intrazona en el centro de datos en estas tres zonas internas del centro de datos.

STEP 1 | Seleccione la fila intrazone-default (intrazona-predeterminada) en la base de reglas y haga clic en **Override (Cancelar)** para habilitar la edición en esta regla.

STEP 2 | Seleccione el nombre de la regla **intrazone-default (intrazona-predeterminada)** para editar la regla.

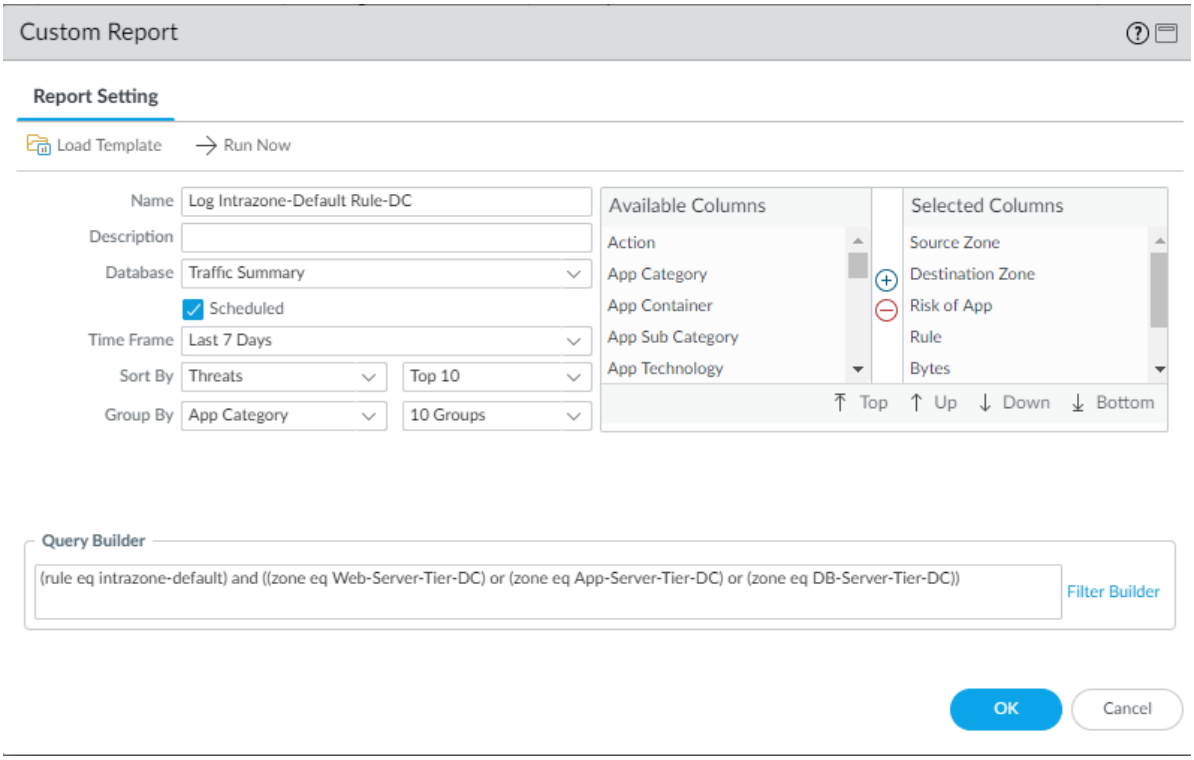
STEP 3 | En la pestaña Actions (Acciones), seleccione **Log at Session End (Log al finalizar sesión)** y haga clic en **OK (Aceptar)**.

STEP 4 | Cree un informe personalizado para supervisar el tráfico que coincide con esta regla para las zonas internas del centro de datos.

1. Seleccione **Monitor (Supervisar)** > **Manage Custom Reports (Gestionar informes personalizados)**.
2. Seleccione **Add** para añadir un informe y **Name** para asignarle un nombre descriptivo. En este ejemplo, el nombre es **Log Intrazone-Default Rule-DC**.
3. Configure la **Database (Base de datos)** en **Traffic Summary (Resumen de tráfico)**.
4. De **Available Columns (Columnas disponibles)**, añada **Source Zone (Zona de origen)**, **Destination Zone (Zona de destino)**, **Sessions (Sesiones)**, **Bytes**, **Application (Aplicación)**, **Risk of App (Riesgo de la aplicación)**, **Rule (Regla)** y **Threats (Amenazas)** a la lista **Selected Columns (Columnas seleccionadas)**. Si desea supervisar otros tipos de información, selecciónelos.
5. Seleccione la casilla de verificación **Scheduled (Programado)**.
6. Configure los valores de **Time Frame (Periodo)**, **Sort By (Ordenar por)** y **Group By (Agrupar por)** que desee. En este ejemplo, los valores seleccionados son **Threats (Amenazas)** y **App Category (Categoría de aplicación)**, respectivamente.
7. Defina la consulta para que coincida con el tráfico que corresponda a la regla intrazone-default (intrazona-predeterminada):

```
(rule eq intrazone-default) and ((zone eq Web-Server-Tier-DC) or (zone eq
 App-Server-Tier-DC) or (zone eq DB-Server-Tier-DC))
```

La consulta filtra el tráfico que coincide con la regla de interzona predeterminada y con alguna de las tres zonas internas del centro de datos que se definieron. Dado que las **Selected Columns (Columnas seleccionadas)** predeterminadas incluyen las zonas, el informe muestra la zona de cada sesión. En un centro de datos real, probablemente, tendría más zonas y añadiría cada zona a la consulta. Los ajustes finales del informe personalizado son los siguientes:



8. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

Registro del tráfico en el centro de datos que no coincide con reglas en la interzona

El tráfico que no coincide con ninguna de las reglas en la política de seguridad que configuró coincide con la regla de bloqueo interzone-default en la parte inferior de la base de reglas y se bloqueará. Para obtener visibilidad del tráfico que no coincide con una regla que configuró explícitamente, habilite la generación de logs en la regla interzone-default (interzona-predeterminada). El registro del tráfico le permite examinar los intentos de acceso que no permitió explícitamente, lo que puede identificar los posibles ataques o el tráfico por el cual quizás desee modificar una regla de permiso.

STEP 1 | Seleccione la fila interzone-default (interzona-predeterminada) en la base de reglas y haga clic en **Override (Cancelar)** para habilitar la edición en esta regla.

STEP 2 | Seleccione el nombre de la regla **interzone-default (interzona-predeterminada)** para editar la regla.

STEP 3 | En la pestaña Actions (Acciones), seleccione **Log at Session End (Log al finalizar sesión)** y haga clic en **OK (Aceptar)**.

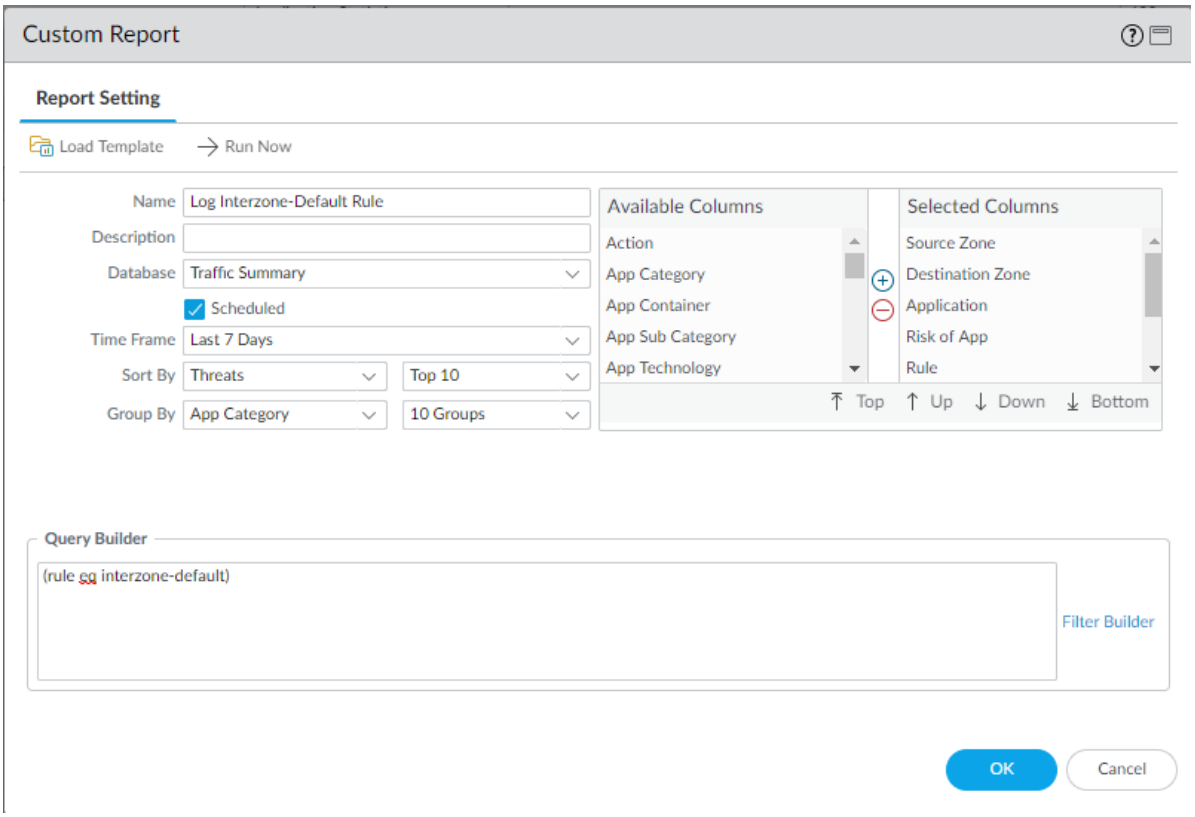
STEP 4 | Cree un informe personalizado para supervisar el tráfico que coincida con esta regla.

1. Seleccione **Monitor (Supervisar)** > **Manage Custom Reports (Gestionar informes personalizados)**.
2. Seleccione **Add** para añadir un informe y **Name** para asignarle un nombre descriptivo. En este ejemplo, el nombre es **Log Interzone-Default Rule**.
3. Configure la **Database (Base de datos)** en **Traffic Summary (Resumen de tráfico)**.

4. De **Available Columns (Columnas disponibles)**, añada **Source Zone (Zona de origen)**, **Destination Zone (Zona de destino)**, **Sessions (Sesiones)**, **Bytes**, **Application (Aplicación)**, **Risk of App (Riesgo de la aplicación)**, **Rule (Regla)** y **Threat (Amenaza)** a la lista **Selected Columns (Columnas seleccionadas)**. Si desea supervisar otros tipos de información, selecciónelos.
5. Seleccione la casilla de verificación **Scheduled (Programado)**.
6. Configure los valores de **Time Frame (Periodo)**, **Sort By (Ordenar por)** y **Group By (Agrupar por)** que desee. En este ejemplo, los valores seleccionados son **Last 7 Days (Últimos 7 días)**, **Threats (Amenazas)** y **App Category (Categoría de aplicación)**, respectivamente.
7. Defina la consulta para que coincida con el tráfico que corresponda a la regla interzone-default (interzona-predeterminada):

```
(rule eq interzone-default)
```

Los ajustes finales del informe personalizado son los siguientes:



8. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

Mantenimiento de la base de reglas recomendadas para el centro de datos

Las aplicaciones evolucionan constantemente, de modo que la lista de aplicaciones permitidas debe evolucionar en consecuencia. Debido a que las reglas recomendadas aprovechan objetos de la política para simplificar la administración, incluir la compatibilidad con una nueva aplicación o eliminar una aplicación de la lista de permitidos, en general, implica modificar el grupo de aplicaciones o el filtro de aplicaciones en consecuencia.

Palo Alto Networks envía actualizaciones de contenido que debe descargar automáticamente y programar para que se instalen en el cortafuegos lo antes posible. La mayoría de las actualizaciones de contenido incluyen actualizaciones del contenido de amenazas (antivirus, vulnerabilidades, antispyware, etc.) y pueden contener App-ID modificados. El tercer martes de cada mes, la actualización de contenido también incluye nuevos App-ID. Puede configurar umbrales diferentes para demorar la instalación de actualizaciones de contenido regulares y la instalación de actualizaciones mensuales que contengan nuevas App-ID durante un período de tiempo especificado tras la descarga. Retrasar la instalación le permite instalar las actualizaciones de contenido que no incluyen nuevos App-ID lo antes posible para obtener las firmas de amenazas más recientes, y brinda más tiempo para examinar los nuevos App-ID antes de instalarlos.

Las actualizaciones de contenido en el tercer martes de cada mes que contienen los nuevos App-ID pueden provocar cambios en la aplicación de la política de seguridad. Antes de instalar App-ID nuevos o modificados, revise el impacto de la política, organice las actualizaciones para evaluar el impacto y modifique las reglas existentes en la política de seguridad si es necesario. La manera más eficaz de controlar la descarga y la instalación de las actualizaciones de contenido en los cortafuegos es descargarlas y retirarlas de Panorama si usa Panorama.

Respete las prácticas recomendadas de actualización de contenido generales, pero tenga en cuenta que la disponibilidad del centro de datos es crítica, de modo que es posible que no implemente las actualizaciones de contenido con la misma rapidez en el centro de datos y en los cortafuegos accesibles desde internet:

- Pruebe rápidamente las actualizaciones de contenido en un área segura de la red antes de instalarlas en el centro de datos.
- En el caso de las actualizaciones de contenido que no contienen nuevos App-ID, configure el umbral de instalación en no más de ocho horas tras la descarga automática y realice pruebas en ese período.
- En el caso de las actualizaciones de contenido que contienen nuevos App-ID, configure el umbral de instalación en no más de ocho días tras la descarga automática y realice pruebas en ese período.
- Configure el reenvío de logs en todas las actualizaciones de contenido.

STEP 1 | Antes de instalar una nueva actualización de contenido, revise los App-ID nuevos y modificados para determinar si habrá un impacto en la política.

STEP 2 | Si es necesario, modifique las reglas existentes en la política de seguridad para adaptarse a los cambios del App-ID.

Puede deshabilitar App-ID seleccionados si algunos requieren más pruebas e instalar el resto de los App-ID. Termine de probar las revisiones de la política necesarias antes de la versión de contenido del mes siguiente con los nuevos App-ID (tercer martes de cada mes) para evitar que se superpongan.

Con el tiempo, la lista de aplicaciones que se usan en el centro de datos se estabiliza y cada vez, son menos los App-ID relevantes. (La mayoría de los App-ID nuevos pertenecen a aplicaciones accesibles desde internet). Esto reduce el riesgo de que los

nuevos App-ID causen problemas en el centro de datos y es posible que le permita instalar actualizaciones de contenido con nuevos App-ID con mayor rapidez.

STEP 3 | Prepare actualizaciones de la política para tener en cuenta los cambios de App-ID en una versión de contenido o para añadir nuevas aplicaciones autorizadas a o eliminar aplicaciones de las reglas de permiso.

Otras maneras de mantener una base de reglas recomendada son las siguientes:

- Use las herramientas de evaluación y revisión de Palo Alto Networks para identificar brechas en la cobertura de seguridad.
- Es posible que los reclamos de usuarios acerca de las aplicaciones a las que ya no pueden acceder indiquen brechas en la base de reglas o aplicaciones inseguras que se usaron en la red antes de que la aplicación positiva evitara su uso.
- Compare la lista del inventario de activos que realizó cuando evaluó el centro de datos con los activos reales y garantice que se protejan adecuadamente.
- Use las herramientas generación de logs y supervisión de Palo Alto Networks como el centro de control de aplicaciones (Application Command Center, ACC) para hallar e investigar actividades inesperadas, que podrían indicar una regla faltante o con una configuración errónea. Ejecute informes periódicamente para comprobar que el nivel de seguridad que desea aplicar se aplique.

Si usa Panorama para gestionar los cortafuegos, puede supervisar el estado del cortafuegos para comparar los dispositivos con el rendimiento de referencia y entre sí para identificar las desviaciones del comportamiento normal.

Uso de las herramientas de evaluación y revisión de Palo Alto Networks

El equipo de éxito del cliente de Palo Alto Networks desarrolló una arquitectura de prevención con herramientas y recursos que ayudan a revisar y evaluar los riesgos de seguridad de la red, y determinar la eficacia del uso de las capacidades del cortafuegos y otras herramientas para proteger la red. Comuníquese con el representante de Palo Alto Networks para programar evaluaciones y revisiones (un ingeniero de ventas de Palo Alto Networks realiza las revisiones para brindar experiencia en la evaluación del estado de seguridad de la red). Al momento de esta publicación, las herramientas de prevención de riesgos de seguridad disponibles incluyen las siguientes:

- **Evaluación de la postura de prevención (Prevention Posture Assessment, PPA)**: la PPA consiste en un conjunto de cuestionarios que permiten hallar brechas en la prevención de riesgos de seguridad en todas las áreas de la red y la arquitectura de seguridad. La PPA no solo permite identificar todos los riesgos de seguridad, también brinda sugerencias detalladas sobre cómo prevenir los riesgos y cerrar las brechas. La evaluación, guiada por un ingeniero de ventas de Palo Alto Networks experimentado, permite determinar las áreas de mayor riesgo donde debe centrar las actividades de prevención. Puede ejecutar la PPA en los cortafuegos y en Panorama.
- **Herramienta de evaluación recomendada (Best Practice Assessment, BPA):** la BPA para los cortafuegos de última generación y Panorama evalúa la configuración de un dispositivo midiendo la adopción de capacidades, validando si las políticas respetan las prácticas recomendadas y brindando recomendaciones e instrucciones sobre cómo solucionar las comprobaciones recomendadas fallidas.

  El mapa de calor de adopción de la política de seguridad filtra la información por grupos de dispositivos, números de serie, zonas, áreas de arquitectura y otras categorías. Los resultados incluyen datos de tendencias, que muestran la tasa de mejora de seguridad a medida que adopta nuevas capacidades, soluciona brechas y progresa hacia una red de confianza cero.

  El componente de BPA realiza más de 200 comprobaciones de seguridad en un cortafuegos o configuración de Panorama, y brinda un puntaje aprobado/fallido a cada comprobación. Cada comprobación forma parte de las prácticas recomendadas de los expertos en seguridad de Palo Alto Networks. Si el resultado de una comprobación es un puntaje fallido, la herramienta brinda la justificación del resultado y cómo resolver el problema.

Palo Alto Networks continúa desarrollando nuevas herramientas y mejorando las herramientas existentes. Comuníquese con el representante de Palo Alto Networks para descubrir lo que pueden hacer las herramientas más recientes para aumentar la seguridad de la red del centro de datos.